Pro-endliche Gruppen[1]

Franz Lemmermeyer
hb3@ix.urz.uni-heidelberg.de

4. August 1999

[1]Zweistündige Vorlesung an der Universität Bonn, Sommersemester 1999.

Inhaltsverzeichnis

1 Galoistheorie unendlicher Erweiterungen **3**
- 1.1 Topologische Gruppen 6
- 1.2 Die Krullsche Topologie 8
- 1.3 Der Hauptsatz der Galoistheorie 9
- 1.4 Bemerkungen 12

2 Projektive Limites **19**
- 2.1 Galoisgruppen 19
- 2.2 Funktorielle Eigenschaften des projektiven Limes 23
- 2.3 Eigenschaften pro-endlicher Gruppen 28

3 Kohomologiegruppen niedriger Dimension **33**
- 3.1 Diskrete G-Moduln 33
- 3.2 Das Schlangenlemma 35
- 3.3 Die erste Kohomologiegruppe 37
- 3.4 Die Tateschen Gruppen $\widehat{\mathrm{H}}^0$ und $\widehat{\mathrm{H}}^{-1}$ 46
- 3.5 Geschlechtertheorie quadratischer Zahlkörper 47

4 Die lange Kohomologiesequenz **53**
- 4.1 Die lange exakte Kohomologiesequenz 53
- 4.2 Inflation und Restriktion 60
- 4.3 Induzierte Moduln 63
- 4.4 Direkte Limites von Kohomologiegruppen 67

Kapitel 1

Galoistheorie unendlicher Erweiterungen

Problemstellung

Wir beginnen damit, einige Begriffe der Galoistheorie zu wiederholen. Sei L/K eine Körpererweiterung. Ein $\alpha \in L$ heißt *algebraisch* über K, wenn es ein (oBdA normiertes[1]) Polynom $f \in K[X]$ gibt mit $f(\alpha) = 0$; ist f irreduzibel in $K[X]$, so heißt es Minimalpolynom. Weiter nennt man ein algebraisches $\alpha \in L$ separabel, wenn die Nullstellen des Minimalpolynoms alle einfach sind; Standardbeispiel eines nicht separablen Elements ist $\alpha = T^{1/p}$ über $K = \mathbb{F}_p[T]$: dessen Minimalpolynom ist ersichtlich $X^p - T \in K[X]$, und wegen $X^p - T = (X - \alpha)^p$ ist α eine p-fache Nullstelle.

Die Erweiterung L/K heißt algebraisch (separabel), wenn jedes $\alpha \in L$ algebraisch (separabel) über K ist. Jede endliche Erweiterung eines endlichen Körpers oder von $\mathbb{Q}$ ist separabel. Schließlich nennt man L/K *normal*, wenn die Erweiterung algebraisch ist und jedes in K irreduzible Polynom, welches in L eine Nullstelle hat, über L in Linearfaktoren zerfällt. Ist L/K normal, so nennt man die Gruppe $\mathrm{Gal}\,(L/K)$ aller Automorphismen von L, welche K elementweise fest lassen, die Galoisgruppe von L/K. Man nennt die Erweiterung galoissch, wenn sie normal und separabel ist. Bekanntlich gilt

Proposition 1.1. *Ist L/K normal und separabel, so ist K der Fixkörper von* $\mathrm{Gal}\,(L/K)$.

Um dies zu beweisen, müssen wir für jedes $\alpha \in L \setminus K$ einen Automorphismus $\sigma \in \mathrm{Gal}\,(L/K)$ konstruieren mit $\sigma(\alpha) \neq \alpha$. Dazu brauchen wir bloß einen entsprechenden Isomorphismus von $K(\alpha)$ "hochzuheben". Das wiederum geschieht mit den nächsten beiden Lemmata.

[1] d.h. der Koeffizient des Termes höchsten Grades ist 1.

Lemma 1.2. *Sei L/K galoissch und $\sigma : L \longrightarrow L$ ein K-Isomorphismus. Dann ist $\sigma \in \mathrm{Gal}\,(L/K)$.*

Beweis. Zu zeigen ist, daß der K-Isomorphismus ein Automorphismus von L, d.h. surjektiv ist. Da jedes $\alpha \in L$ in einem endlichen normalen Teilkörper liegt, genügt es zu zeigen, daß die Einschränkung von σ auf jede endliche normale Teilerweiterung von L/K surjektiv ist. Das folgt aber aus der endlichen Galoistheorie. □

Lemma 1.3. *Sei L/k galoissch, K ein Zwischenkörper von L/k, und $\sigma : K \longrightarrow L$ ein k-Isomorphismus. Dann existiert ein $\widetilde{\sigma} \in \mathrm{Gal}\,(L/k)$ mit $\widetilde{\sigma}|_K = \sigma$.*

Beweis. Sei S die Menge aller Paare (F, ρ) mit $K \subseteq F \subseteq L$, sodaß $\rho : K \longrightarrow L$ ein k-Isomorphismus ist. Wegen $(L, \sigma) \in S$ ist S nicht leer. Wir führen auf S eine partielle Ordnung ein durch $(F_1, \rho_1) \leq (F_2, \rho_2)$ falls $F_1 \subseteq F_2$ und $\rho_2|_{F_1} = \rho_1$. Wir behaupten, daß S damit induktiv geordnet ist, d.h. daß jede total geordnete Teilmenge $\{(F_i, \rho_i)\}$ ein Maximum besitzt. Dazu setzen wir $\widetilde{F} := \cup_i F_i$ und definieren einen Automorphismus $\widetilde{\rho}$ von F durch $\widetilde{\rho}(\alpha) = \rho_i(\alpha)$, wenn $\alpha \in F_i$ ist. Wegen der Totalordnung ist dies wohldefiniert.

Nach dem Lemma von Zorn besitzt dann S ein maximales Element $(L', \widetilde{\sigma})$. Wir behaupten, daß $L' = L$ gilt. Andernfalls gäbe es nämlich ein $\alpha \in L \setminus L'$, und wir könnten den Automorphismus $\widetilde{\sigma}$ auf $L'(\alpha)$ hochheben: das widerspricht aber der Maximalität von $(L', \widetilde{\sigma})$. □

Ist L/K eine endliche galoissche Erweiterung, so stellt der Hauptsatz der Galoistheorie eine ordnungsumkehrende Bijektion zwischen Untergruppen von $\mathrm{Gal}\,(L/K)$ und Teilkörpern von L/K her. Für unendliche normale Erweiterungen ist dies falsch, wie das folgende Beispiel zeigt.

Beispiel. Sei $K = \mathbb{F}_p$ der Körper mit p Elementen, und $\mathbb{F} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ sein algebraischer (= separabler) Abschluß. Offensichtlich ist $\mathbb{F}/\mathbb{F}_p$ normal; sei $G = \mathrm{Gal}\,(\mathbb{F}/\mathbb{F}_p)$ seine Galoisgruppe. Dieses enthält den Frobeniusautomorphismus $\phi : \alpha \longmapsto \alpha^p$; sei $H = \langle \phi \rangle$ die von ϕ erzeugte Untergruppe. Jetzt gilt:

1. Der Fixkörper von G ist $\mathbb{F}_p$;
2. Der Fixkörper von H ist $\mathbb{F}_p$;
3. $H \neq G$.

Insbesondere gibt es zwei voneinander verschiedene Untergruppen von G mit demselben Fixkörper.

Nun zum Beweis der Behauptungen. Sei $\alpha \in \mathbb{F}$ und $\phi(\alpha) = \alpha$, also α Nullstelle von $X^p - X \in \mathbb{F}_p[X]$. Dieses Polynom hat die p Elemente von $\mathbb{F}_p$ als Nullstellen; da $\mathbb{F}_p$ ein Körper ist, sind dies schon alle, und es folgt $\alpha \in \mathbb{F}_p$. Das zeigt 2. Wegen $H \subseteq G$ folgt daraus 1. Zum Beweis von 3 müssen wir ein $\tau \in \mathrm{Gal}\,(\mathbb{F}/\mathbb{F}_p)$ konstruieren, das keine Potenz von ϕ ist.

Die Idee ist einfach: wir konstruieren uns einen geeigneten Körper L mit $\mathbb{F}_p \subset L \subsetneq \mathbb{F}$ und wählen ein $\tau \in \mathrm{Gal}\,(\mathbb{F}/L) \setminus \{1\}$. Wäre $H = G$, so folgte $\tau = \phi^n$ für ein $n \in \mathbb{N}$ (notfalls ersetze man τ durch τ^{-1}); also ließe ϕ^n den Körper L elementweise fest, und L wäre im Fixkörper $\mathbb{F}_{p^n}$ von ϕ^n enthalten. Dies liefert einen Widerspruch, falls L unendlich viele Elemente enthält.

Unsere Aufgabe ist es daher, einen echten Teilkörper von $\mathbb{F}$ mit unendlich vielen Elementen zu konstruieren. Das ist aber einfach: man nehme die Erweiterung $L = \bigcup_{n\geq 0} \mathbb{F}_{p^{2^n}}$. □

Bei obigem Beweis haben wir stillschweigend einige Aussagen der Galoistheorie benutzt, deren Beweis wir noch nachzutragen haben. Zum einen haben wir benutzt, daß $\mathbb{F}/L$ galoissch ist; dies folgt aus

Lemma 1.4. *Ist K ein Zwischenkörper der algebraischen (normalen, separablen, galoisschen) Erweiterung L/F, so ist auch L/K algebraisch (normal, separabel, galoissch).*

Beweis. Daß L/K algebraisch ist, ist offensichtlich wegen $F[X] \subset K[X]$. Sei nun L/F normal und $f \in K[X]$ irreduzibel. Ist dann $\alpha \in L$ eine Nullstelle von f, so ist zu zeigen, daß f in L in Linearfaktoren zerfällt. Sei dazu $h \in F[X]$ das Minimalpolynom von α über F. Der euklidische Algorithmus in $K[X]$ gibt $h = fq + r$ für ein $r \in K[X]$ mit $\deg r < \deg f$; außerdem ist $r(\alpha) = 0$. Daraus folgt aber mit der Irreduzibilität von f, daß $r = 0$ ist, und somit ist f Teiler von h. Da aber h in L in Linearfaktoren zerfällt, folgt die Behauptung. Genauso behandelt man die Separabilität, und wegen galoissch = normal und separabel ist alles gezeigt. □

Zweitens haben wir folgende Tatsache verwendet:

Lemma 1.5. *Sei $F_0 \subset F_1 \subset F_2 \subset \ldots$ eine Folge von quadratischen Erweiterungen und L/F_0 eine kubische Erweiterung. Dann ist L nicht in $F_\infty = \bigcup_{n\geq 0} F_n$ enthalten.*

Beweis. Sei $L = F(\alpha)$; wäre $\alpha \in F_\infty$, so gäbe es ein $n \in \mathbb{N}$ mit $\alpha \in F_n$. Aber $(F_n : F) = 2^n$ ist nicht durch $3 = (L : F)$ teilbar. □

Das obige Problem beim Hauptsatz der Galoistheorie für unendliche Erweiterungen L/K kommt daher, daß es Gruppen H gibt, deren Fixkörper gleich K ist, ohne daß H schon die ganze Galoisgruppe ist. Die Frage, wie man den Hauptsatz abzuändern hat, hat Krull Ende der 20er Jahren beantwortet: man topologisiert die Galoisgruppe und erhält dann eine Bijektion zwischen *abgeschlossenen Untergruppen* der Galoisgruppen und den Teilkörpern der Erweiterung. In unserem obigen Beispiel ist der Abschluß der von ϕ erzeugten Gruppe schon die ganze Galoisgruppe, und alles löst sich in Wohlgefallen auf.

1.1 Topologische Gruppen

Eine Menge G, die mit einer Gruppenstruktur und einer Topologie versehen ist, heißt *topologische Gruppe*, wenn sich Topologie und Gruppenstruktur vertragen; genauer sollen Multiplikation und Inversenbildung *stetige* Abbildungen sein, d.h. es wird verlangt:

- Die Abbildung $G \times G \longrightarrow G : (x, y) \longmapsto xy$ ist stetig, wobei $G \times G$ mit der Produkttopologie versehen ist;
- Die Abbildung $G \longrightarrow G : x \longmapsto x^{-1}$ ist stetig.

Beispiele für topologische Gruppen gibt es unzählige: jede (endliche) Gruppe ist, versehen mit der diskreten Topologie, eine topologische Gruppe. Die additive Gruppe der rationalen (reellen, komplexen) Zahlen ist eine topologische Gruppe bezüglich der gewöhnlichen Topologie, die von der euklidischen Metrik induziert wird. Daneben ist $\mathbb{Q}$ auch topologische Gruppe bezüglich der p-adischen Topologien. Weiter ist $\mathbb{R}^\times$ mit der üblichen Metrik eine topologische Gruppe, und was wegen $\mathbb{R}^\times = \mathrm{GL}_1(\mathbb{R})$ für $n = 1$ gilt, kann man natürlich auch auf $\mathrm{GL}_n(\mathbb{R})$ übertragen.

Übung. Man versehe $\mathbb{Z}$ mit folgender Topologie: eine Teilmenge $X \subseteq \mathbb{Z}$ heiße offen, wenn $0 \notin \mathbb{Z}$ oder $\mathbb{Z} \setminus X$ endlich ist. Man überzeuge sich davon, daß dies wirklich eine (hausdorffsche) Topologie ist, und daß $\mathbb{Z}$ mit dieser Topologie keine topologische Gruppe bildet.

Bemerkung. Man versehe $\mathbb{Z}$ mit der Topologie, deren Basis die arithmetischen Progressionen bilden. Eine Menge $U \subseteq \mathbb{Z}$ ist daher offen, wenn jedes ihrer Elemente in einer ganz in U liegenden arithmetischen Progression vorkommt. Jede offene Menge ist damit abgeschlossen, weil das Komplement einer arithmetischen Progression die Vereinigung endlich vieler solcher ist. Man betrachte nun die Mengen $A_p = p\mathbb{Z}$, wo p eine Primzahl ist; diese sind offen und abgeschlossen. Die Vereinigung aller A_p ist $\mathbb{Z} \setminus \{\pm 1\}$; da diese Menge nicht offen ist, ist $\bigcup A_p$ nicht abgeschlossen. Also kann $\bigcup A_p$ nicht die Vereinigung endlich vieler A_p sein, folglich muß es unendlich viele Primzahlen geben.

Die Literatur über topologische Gruppen ist immens; glücklicherweise kommen wir mit ganz wenig aus:

Lemma 1.6. *Sei G topologische Gruppe und $L_a : G \longrightarrow G$ die Multiplikation mit $a \in G$ von links. Dann ist L_a Homöomorphismus. Insbesondere ist eine Teilmenge $A \subseteq G$ genau dann offen (abgeschlossen), wenn aA dies ist.*

Beweis. Die Homomorphieeigenschaft von L_a ist klar, die Stetigkeit folgt daraus, daß L_a die Komposition der beiden stetigen Abbildungen $G \longrightarrow G \times G : g \longmapsto (a, g)$ und von $G \times G \longrightarrow G : (a, g) \longmapsto ag$ ist. Die Umkehrabbildung $L_{a^{-1}}$ ist aus demselben Grund stetig. □

Lemma 1.7. *Sei G topologische Gruppe und $A, B \subseteq G$ Teilmengen von G. Dann ist $\overline{A} \cdot \overline{B} \subseteq \overline{AB}$, $\overline{A}^{-1} = \overline{A^{-1}}$, und $g\overline{A} = \overline{gA}$ für jedes $g \in G$.*

Beweis. Sei $x \in \overline{A}$ und $y \in \overline{B}$, und sei U eine Umgebung von xy. Wegen der Stetigkeit der Multiplikation gibt es eine Umgebung V der 1, sodaß $xV \cdot yV \subseteq xyU$ gilt. Da x im Rand von A liegt, gibt es ein $a \in xV \cap A$, und analog ein $b \in yV \cap B$. Dann ist $ab \in AB \cap xyU$, d.h. jede Umgebung von xy schneidet AB. Also ist $xy \in \overline{AB}$.

Zum Beweis von $\overline{A}^{-1} = \overline{A^{-1}}$ betrachten wir den Homöomorphismus $I : G \longrightarrow G : g \longmapsto g^{-1}$. Wegen $A^{-1} \subseteq \overline{A}^{-1} = I(\overline{A})$ ist die rechte Seite abgeschlossen, folglich muß auch $\overline{A^{-1}} \subseteq \overline{A}^{-1}$ sein. Andererseits ist $A^{-1} \subseteq \overline{A^{-1}}$, somit $A \subseteq \overline{A^{-1}}^{-1} = I(\overline{A^{-1}})$. Wieder ist die rechte Seite abgeschlossen, also $\overline{A} \subseteq \overline{A^{-1}}^{-1}$ und damit $\overline{A}^{-1} \subseteq \overline{A^{-1}}$.

Schließlich zu $g\overline{A} = \overline{gA}$. Wegen $gA \subseteq g\overline{A}$ muß $\overline{gA} \subseteq g\overline{A}$ sein (dasselbe Argument wie eben, nur daß statt I der Homöomorphismus L_g verwendet wird). Umgekehrt folgt aus $A \subseteq g^{-1}\overline{gA}$ wieder $\overline{A} \subseteq g^{-1}\overline{gA}$ und damit $g\overline{A} \subseteq \overline{gA}$. □

Proposition 1.8. *Sei G topologische Gruppe und H eine Untergruppe von G. Dann ist H bezüglich der Relativtopologie eine topologische Gruppe, und die Einbettung $H \hookrightarrow G$ ist stetig. Mit H ist auch der topologische Abschluß $\overline{H}$ von H eine Untergruppe von G.*

Beweis. Die Multiplikation $H \times H \longrightarrow H$ ist als Einschränkung einer stetigen Abbildung ebenfalls wieder stetig, und dasselbe gilt für Bildung des Inversen. Zu zeigen ist lediglich, daß $\overline{H}$ eine Gruppe bildet. Nach dem obigen Lemma ist aber $\overline{H} \cdot \overline{H} \subseteq \overline{H \cdot H} = \overline{H}$ und $\overline{H}^{-1} = \overline{H^{-1}} = \overline{H}$, somit $\overline{H}$ eine Gruppe. □

Proposition 1.9. *Offene Untergruppen topologischer Gruppen sind gleichzeitig abgeschlossen.*

Beweis. Es ist offenbar $G \setminus H = \bigcup_{g \notin H} gH$; da mit H auch alle gH offen sind, ist $G \setminus H$ offen. Also ist H abgeschlossen. □

Übung. Sei G topologische Gruppe und H eine Untergruppe von G. Zeige: Ist G hausdorffsch und H abelsch, dann ist auch $\overline{H}$ abelsch.

Es folgen noch einige Bemerkungen zur Topologie von Faktorgruppen. Sei $(G, \mathcal{O})$ eine topologische Gruppe, $H \leq G$ eine Untergruppe, G/H die Menge der Linksnebenklassen, und $\phi : G \longrightarrow G/H$ die kanonische Projektion. Dann wird durch $\mathcal{O}' = \{U \subseteq G/H : \phi^{-1}(U) \in \mathcal{O}\}$ eine Topologie auf G/H definiert, bezüglich der ϕ stetig und offen ist. In der Tat sind $\varnothing$ und G/H offen wegen $\varnothing = \phi^{-1}(\varnothing)$ und $G = \phi^{-1}(G/H)$. Sind weiter $A_i \in \mathcal{O}'$, also $\phi^{-1}(A_i) \in \mathcal{O}$, so ist $\phi^{-1}(\bigcup A_i) = \bigcup \phi^{-1}(A_i) \in \mathcal{O}$ und damit $\bigcup A_i \in \mathcal{O}'$. Ebenso folgt, daß der Durchschnitt endlich vieler offener Mengen wieder offen ist. Weiter ist ϕ

per definitionem stetig, und zum Beweis der Offenheit sei $U \in \mathcal{O}$; dann ist $\phi^{-1}(\phi(U)) = UH$. Mit U ist aber auch UH offen.

Sei ab jetzt H ein Normalteiler von G. Dann ist G/H eine Gruppe, die wir eben mit einer Topologie versehen haben. In der Tat wird G/H damit zur topologischen Gruppe. Um die Stetigkeit der Multiplikation einzusehen, sei W eine Umgebung von $g_1 g_2 H \in G/H$. Dann ist $\phi^{-1}(W)$ eine offene Umgebung von $g_1 g_2$, und nach der Stetigkeit der Multiplikation in G existieren Umgebungen U_j von g_j mit $U_1 U_2 \subseteq \phi^{-1}(W)$. Da ϕ offen ist, sind dann $\phi(U_j)$ Umgebungen von $g_j H$, und es ist $\phi(U_1)\phi(U_2) = \phi(U_1 U_2) \subseteq W$. Die Stetigkeit der Inversenbildung folgt analog, und wir haben gezeigt:

Proposition 1.10. *Ist H Normalteiler einer topologischen Gruppe, so wird G/H mit der Quotiententopologie ebenfalls zu einer topologischen Gruppe, und die kanonische Projektion $\phi : G \longrightarrow G/H$ ist stetig und offen.*

Damit haben wir folgende topologische Version eines bekannten Isomorphiesatzes:

Proposition 1.11. *Seien G_1, G_2 topologische Gruppen und $\pi : G_1 \longrightarrow G_2$ ein offener und stetiger Epimorphismus. Dann induziert $\overline{\pi} : G_1/\ker\pi \longrightarrow G_2$ einen topologischen Isomorphismus $G_1/\ker\pi \simeq G_2$.*

Beweis. Daß $\overline{\pi}$ Gruppenisomorphismus ist, ist klar. Zu zeigen ist, daß $\overline{\pi}$ stetig und offen ist. Sei dazu $U_2 \subseteq G_2$ offen; da π stetig ist, ist $\pi^{-1}(U_2)$ offen in G_1, folglich $\overline{\pi}^{-1}(U_2) = \phi(\pi^{-1}(U_2))$ offen, weil ϕ offen ist. Also ist $\overline{\pi}$ stetig.

Sei nun $U \subseteq G_1/\ker\pi$ offen. Dann ist $U_1 := \phi^{-1}(U)$ offen in G_1, also $\overline{\pi}(U) = \pi(U_1)$ offen in G_2, weil π offen ist. □

1.2 Die Krullsche Topologie

Sei L/K galoissch; die Menge

$$\mathcal{O} = \{\mathrm{Gal}\,(L/F) : F/K \text{ ist endlich und normal}\}$$

definiert eine Umgebungsbasis der 1. Mit anderen Worten: eine Menge $U \subseteq G = \mathrm{Gal}\,(L/K)$ ist offen, wenn es zu jedem $\sigma \in G$ eine endliche normale Erweiterung F/K gibt, sodaß $\sigma\,\mathrm{Gal}\,(L/F) \subseteq U$ gilt.

Ist L/K endlich, so ist jedes Element von G offen (man braucht ja nur immer $H = \mathrm{Gal}\,(L/L) = \{1\}$ zu wählen).

Beginnen wir nun mit dem Nachweis, daß $\mathcal{O}$ eine Topologie definiert. Zuerst einmal sind $\varnothing$ und G offen. Sind weiter $H_i = \mathrm{Gal}\,(L/F_i) \in \mathcal{O}$ für $i = 1, 2$, so ist $H_1 \cap H_2 = \mathrm{Gal}\,(L/F_1F_2) \in \mathcal{O}$, da mit F_1 und F_2 auch das Kompositum F_1F_2 eine endliche normale Erweiterung von K ist. Ist $\{H_i\}$ eine ganze Familie solcher offener Untergruppen von G, so ist $\bigcup_i H_i = \mathrm{Gal}\,(L/\bigcap F_i) \in \mathcal{O}$, da der Durchschnitt beliebig vieler endlicher normaler Erweiterungen von K wieder eine solche ist. Damit ist $\mathrm{Gal}\,(L/K)$ ein topologischer Raum.

Ist $\mathrm{Gal}\,(L/K)$ aber auch eine topologische Gruppe? Dazu müssen wir die Verträglichkeit der Topologie mit der Gruppenoperation nachweisen. Betrachten wir also die Abbildung $i : \sigma \longmapsto \sigma^{-1}$. Um die Stetigkeit nachzuweisen, genügt es zu zeigen, daß das Urbild der offenen Basisumgebung $H = \mathrm{Gal}\,(L/F)$ mit F/K endlich und normal wieder eine offene Menge enthält. Weil aber H eine Gruppe ist, ist $i^{-1}(H) = H$ und damit alles klar. Die Stetigkeit der Multiplikation folgt ebenso leicht: sei $H = \sigma\tau\,\mathrm{Gal}\,(L/F)$ eine offene Basisumgebung von $\sigma\tau$. Dann sind σH und τH offene Umgebungen von σ bzw. τ, und es ist $\sigma H \cdot \tau H = \sigma\tau H \cdot H = \sigma\tau H$. Dabei haben wir erstens benutzt, daß H Normalteiler von G ist, und zweitens, daß wegen der Gruppeneigenschaft $H \cdot H = H$ gilt.

Also ist $(G, \mathcal{O})$ topologische Gruppe. Als nächstes behaupten wir, daß die Topologie hausdorffsch ist. Seien dazu $\sigma, \tau \in G$ mit $\sigma \neq \tau$. Gesucht sind $U, V \in \mathcal{O}$ mit $\sigma U \cap \tau V = \varnothing$. Dazu wählen wir ein $\alpha \in L$ mit $\sigma(\alpha) \neq \tau(\alpha)$; dann ist der normale Abschluß F von $K(\alpha)$ eine endliche normale Erweiterung von K, somit $H = \mathrm{Gal}\,(L/F) \in \mathcal{O}$. Wäre $\sigma H \cap \tau H$ nicht leer, so folgte $\sigma \in \tau H$: das kann aber nicht sein, da H den Körper F elementweise fest läßt, andererseits $\alpha \in F$ gilt.

Damit ist $\mathrm{Gal}\,(L/K)$ für jede Galoiserweiterung eine hausdorffsche topologische Gruppe. Wenn nicht ausdrücklich anders erwähnt, wird im folgenden $\mathrm{Gal}\,(L/K)$ immer mit der Krullschen Topologie versehen sein. Weiter ist einfach einzusehen, daß $\mathrm{Gal}\,(L/K)$ total unzusammenhängend ist, während der Nachweis, daß $\mathrm{Gal}\,(L/K)$ kompakt ist, etwas mehr Mühe bereitet (für einen direkten Beweis siehe Artin [2]; Lorenz [8] benutzt den Satz von Tychonoff plus die Interpretation von $\mathrm{Gal}\,(L/K)$ als projektiver Limes, McCarthy [10] dagegen Ultrafilter und Bourbaki. Da wir die Kompaktheit demnächst in einer allgemeineren Situation via Tychonoff bekommen werden, verzichten wir hier auf den Beweis; für den Hauptsatz der Galoistheorie ist dieses Wissen ohnehin nicht erforderlich.

1.3 Der Hauptsatz der Galoistheorie

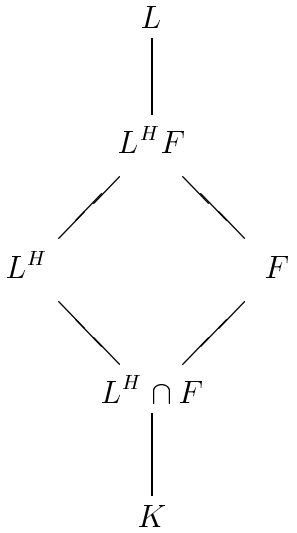
Zur Formulierung des Krullschen Hauptsatzes der Galoistheorie definieren wir bei gegebener galoisscher Körpererweiterung L/K Abbildungen Φ und Ψ durch $\Phi(F) = \mathrm{Gal}\,(L/F)$ für Zwischenerweiterungen F/K von L/K und $\Psi(H) = L^H := \{\alpha \in L : \alpha^\sigma = \alpha\ \forall \sigma \in H\}$ für Untergruppen H von $G = \mathrm{Gal}\,(L/K)$. Der Hauptsatz der endlichen Galoistheorie besagt, daß $\Phi \circ \Psi$ und $\Psi \circ \Phi$ die identischen Abbildung sind. Die letztere der beiden Relationen gilt aus formalen Gründen und ist daher auch für unendliche Galoiserweiterungen richtig: ist nämlich $K \subseteq F \subseteq L$, so gilt $\Psi(\Phi(F)) = \Psi(\mathrm{Gal}\,(L/F))$, und das ist die Menge aller $\alpha \in L$, welche von $\mathrm{Gal}\,(L/F)$ fest gelassen werden. Da mit L/K auch L/F galoissch ist, ist der Fixkörper von $\mathrm{Gal}\,(L/F)$ aber F. Die Bezie-

hung $\Phi \circ \Psi = \mathrm{id}$ ist dagegen für unendliche Erweiterungen nur dann richtig, wenn man G mit der Krullschen Topologie versieht und Ψ auf abgeschlossene Untergruppen einschränkt.

Satz 1.12. *Sei L/K eine (endliche oder unendliche) Galoiserweiterung mit $G = \mathrm{Gal}\,(L/K)$. Die Abbildung Φ, die einem Zwischenkörper F die Gruppe $\mathrm{Gal}\,(L/F)$ zuordnet, stiftet eine Bijektion zwischen dem Verband der Zwischenkörper von L/K und den abgeschlossenen Untergruppen von G. Ist H irgendeine Untergruppe von G und F ihr Fixkörper, so ist $\mathrm{Gal}\,(L/F) = \overline{H}$ der topologische Abschluß von H. Weiter ist F/K genau dann normal, wenn $\mathrm{Gal}\,(L/F)$ ein Normalteiler von G ist; in diesem Fall haben wir einen topologischen Isomorphismus $\mathrm{Gal}\,(F/K) \simeq \mathrm{Gal}\,(L/K)/\mathrm{Gal}\,(L/F)$, wenn die Faktorgruppe mit der Quotiententopologie versehen wird.*

Beweis. Wir beginnen mit dem Nachweis, daß $\mathrm{Gal}\,(L/F) = \Phi(F)$ abgeschlossen ist (ist F/K endlich, so ist $\mathrm{Gal}\,(L/F)$ sogar offen und damit nichts zu zeigen). Im allgemeinen Fall sei $\sigma \in G \setminus \mathrm{Gal}\,(L/F)$. Dann existiert ein $\alpha \in F$ mit $\alpha^\sigma \neq \alpha$. Sei N der normale Abschluß von $K(\alpha)/K$. Dann ist $U = \mathrm{Gal}\,(L/N)$ offen, und für $\tau \in U$ gilt $\sigma\tau(\alpha) = \sigma(\alpha) \neq \alpha$. Dies impliziert aber $\sigma U \cap \mathrm{Gal}\,(L/F) = \varnothing$.

Als nächstes zeigen wir $\Phi \circ \Psi = \mathrm{id}$, also $\mathrm{Gal}\,(L/L^H) = \overline{H}$. Für offene Untergruppen H ist das übrigens gar kein Problem: dann ist nämlich $H = \mathrm{Gal}\,(L/F)$ für eine endliche Erweiterung F/K, folglich $\Phi\circ\Psi(H) = \Phi\circ\Psi(\Phi(F)) = \Phi(F) = H$. Das Problem besteht darin, dasselbe für alle abgeschlossenen Untergruppen H zu zeigen.



Wegen $H \subseteq \mathrm{Gal}\,(L/L^H)$ und weil $\mathrm{Gal}\,(L/L^H)$ abgeschlossen ist, gilt sicherlich $\overline{H} \subseteq \mathrm{Gal}\,(L/L^H)$, sodaß nur $\mathrm{Gal}\,(L/L^H) \subseteq \overline{H}$ zu zeigen ist. Sei dazu $\sigma \in \mathrm{Gal}\,(L/L^H)$; wir müssen zeigen, daß $\sigma\,\mathrm{Gal}\,(L/F) \cap \overline{H} \neq \varnothing$ ist für jedes endliche normale F/K. Die Idee besteht darin, ein $\tau \in H$ zu finden mit $\sigma|_F = \tau|_F$: dann ist nämlich $\sigma^{-1}\tau \in \mathrm{Gal}\,(L/F)$ und folglich $\tau \in \sigma\,\mathrm{Gal}\,(L/F) \cap \overline{H}$. Dies macht man so: wir betrachten die Restriktion $\pi : \mathrm{Gal}\,(L/L^H) \longrightarrow \mathrm{Gal}\,(L^HF/L^H)$. Der Fixkörper von $\pi(H)$ ist dann immer noch L^H: denn würde $\alpha \in L^HF \setminus L^H$ von jeder Einschränkung eines Automorphismus aus H festgelassen, dann auch von deren Lifts. Also ist L^H der Fixkörper von $\pi(H)$ in der *endlichen* Galoiserweiterung L^HF/L^H. Nach dem Hauptsatz der endlichen Galoistheorie ist damit $\pi(H) = \mathrm{Gal}\,(L^HF/L^H) \simeq \mathrm{Gal}\,(F/F \cap L^H)$. Also entsteht jeder Automorphismus von $F/F \cap L^H$ als Einschränkung eines Automorphismus von H auf F, und insbesondere existiert ein $\tau \in H$ mit $\sigma|_F = \tau|_F$. Das war zu zeigen.

Schließlich müssen wir uns noch um den topologischen Isomorphismus

$$\mathrm{Gal}\,(F/K) \simeq \mathrm{Gal}\,(L/K)/\,\mathrm{Gal}\,(L/F)$$

kümmern, der gelten soll, wenn $L/F/K$ ein galoisscher Turm ist, also L/K und F/K galoissche Erweiterungen sind.

Dazu betrachten wir die Restriktion $\pi : \mathrm{Gal}\,(L/K) \longrightarrow \mathrm{Gal}\,(F/K)$; deren Kern besteht gerade aus $\mathrm{Gal}\,(L/F)$. Um den topologischen Isomorphismus zu bekommen, müssen wir nur nachweisen, daß π offen und stetig ist (vgl. Prop. 1.11). Zur Stetigkeit: sei $H \subseteq \mathrm{Gal}\,(F/K)$ eine offene Basisumgebung der 1, also $H = \mathrm{Gal}\,(F/N)$ mit einer endlichen normalen Teilerweiterung N/K von F/K. Dann ist $\pi^{-1}(\mathrm{Gal}\,(F/N)) = \mathrm{Gal}\,(L/N)$ offen in $\mathrm{Gal}\,(L/K)$, also π stetig. Die Umkehrung gilt aus genau demselben Grund. □

Schließlich geben wir noch eine Charakterisierung der offenen und abgeschlossenen Untergruppen von Galoisgruppen:

Proposition 1.13. *Sei L/K galoissch und $G = \mathrm{Gal}\,(L/K)$; dann sind die offenen Untergruppen von G genau die Gruppen $\mathrm{Gal}\,(L/F)$, wo F/K endlich ist. Die abgeschlossenen Untergruppen sind genau die Durchschnitte offener Gruppen.*

Beweis. Sei F/K endlich, und $\widetilde{F}/K$ der normale Abschluß von F/K in L/K. Dann ist $\mathrm{Gal}\,(L/\widetilde{F}) \subseteq \mathrm{Gal}\,(L/F) \subseteq G$, somit $\mathrm{Gal}\,(L/F) = \bigcup \sigma\,\mathrm{Gal}\,(L/\widetilde{F})$ [die Vereinigung geht über alle $\sigma \in \mathrm{Gal}\,(L/F)$] offen, da alle Nebenklassen $\sigma\,\mathrm{Gal}\,(L/\widetilde{F})$ dies sind.

Sei nun umgekehrt H eine offene Untergruppe von G. Die Offenheit besagt, daß es eine endliche normale Teilerweiterung $\widetilde{F}/K$ von L/K gibt mit $\mathrm{Gal}\,(L/\widetilde{F}) \subseteq H$. Wir betrachten nun den durch die Restriktion von $\sigma \in G$ auf $\widetilde{F}$ definierten Epimorphismus $\pi : G \longrightarrow \mathrm{Gal}\,(\widetilde{F}/K)$. Dann ist $\ker\pi = \mathrm{Gal}\,(L/\widetilde{F})$; weiter ist das Bild $\pi(H)$ als Untergruppe der endlichen Galoisgruppe $\mathrm{Gal}\,(F/K)$ nach dem Hauptsatz der endlichen Galoistheorie gleich einem $\mathrm{Gal}\,(\widetilde{F}/F)$. Nun ist $\pi(\sigma) \in \pi(H)$ genau dann, wenn $\sigma \in H \cdot \ker\pi$ ist; wegen $\ker\pi \subseteq H$ ist dies äquivalent zu $\sigma \in H$. Andererseits besteht $\pi(H)$ aus denjenigen Automorphismen von $\widetilde{F}/K$, die auf F trivial sind. Also folgt $H = \mathrm{Gal}\,(L/F)$.

Nun zu den abgeschlossenen Gruppen. Da offene Gruppen abgeschlossen sind, sind Durchschnitte offener Gruppen abgeschlossen. Ist umgekehrt H eine abgeschlossene Untergruppe von G, so ist H enthalten im Durchschnitt der Gruppen HU, wo U die offenen Untergruppen von G durchläuft. Tatsächlich ist H gleich diesem Durchschnitt: ist nämlich $\sigma \in \bigcap_U HU$, so ist $\sigma U \cap H \neq \varnothing$, folglich $\sigma \in \overline{H} = H$. Da die Untergruppen HU alle offen sind, folgt die Behauptung. □

Noch ein Beispiel

Ein Beispiel einer Galoiserweiterung, an dem das Problem der Verallgemeinerung des Hauptsatzes auf unendliche Erweiterung vielleicht noch leichter zu sehen ist als am algebraischen Abschluß von $\mathbb{F}_p$, ist folgendes: man betrachte

$$L = \mathbb{Q}(\sqrt{\mathbb{N}}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots).$$

Ein Automorphismus von $L/\mathbb{Q}$ ist durch seine Operation auf den $\sqrt{p}$ festgelegt. Sei σ_p derjenige Automorphismus von $L/\mathbb{Q}$, welcher $\sqrt{p}$ auf $-\sqrt{p}$ abblidet und alle $\sqrt{q}$ mit $q \neq p$ festläßt. Sei H die Untergruppe von $G = \mathrm{Gal}\,(L/\mathbb{Q})$, welche von diesen σ_p erzeugt wird. Dann ist klar, daß der Fixkörper von H gleich $\mathbb{Q}$ ist: wird nämlich $\alpha \in L$ von allen σ_p festgelassen, so ist α in einem $K_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ enthalten und wird von allen Einschränkungen der σ_p festgelassen (diese erzeugen offenbar ganz $\mathrm{Gal}\,(K_n/\mathbb{Q})$). Also ist $\alpha \in \mathbb{Q}$.

Andererseits gibt es offensichtlich Automorphismen von $L/\mathbb{Q}$, welche nicht in H enthalten sind: Man betrachte nur das Element τ, welches alle $\sqrt{p}$ auf $-\sqrt{p}$ abbildet: wäre es ein Element von H, so wäre es ein endliches Produkt von σ_p's und könnte deswegen höchstens endlich viele Quadratwurzeln bewegen.

Obwohl die σ_p's also die Galoisgruppe G niemals algebraisch erzeugen können, sind sie doch topologische Erzeugende in dem Sinne, daß $\overline{H} = G$ gilt. Dazu ist nur nachzuweisen, daß es zu jeder offene Umgebung U eines $\sigma \in \overline{H}$ ein $\tau \in U \cap H$ gibt. Das ist aber nicht schwer: oBdA sei $U = \sigma\,\mathrm{Gal}\,(L/K)$ für eine endliche normale Teilerweiterung $K/\mathbb{Q}$ von L/K. Die Einschränkung von σ auf K ist dann Produkt gewisser $\sigma_p|_K$. Dieses Produkt der σ_p ist dann ein Element von H, und es liegt auch in $U = \sigma\,\mathrm{Gal}\,(L/K)$, weil ja der Quotient von σ und dem Produkt der σ_p ein Element von G ist, welches K elementweise festläßt und somit in $\mathrm{Gal}\,(L/K)$ liegt.

Wir können auch leicht einsehen, daß G überabzählbar ist (insbesondere ist Abzählbarkeit keine Eigenschaft, die bei der Bildung des topologischen Abschlusses erhalten bleibt): jedes $\sigma \in G$ ist festgelegt durch seine Operation auf den $\sqrt{p}$; die Elemente $\sigma \in G$ werden also beschrieben durch "Vektoren" $(a_2, a_3, \dots, a_p, \dots)$ mit durch $\sqrt{p}^{\sigma-1} = (-1)^{a_p}$ definierten Elementen $a_p \in \{0, 1\}$, und jeder solche Vektor definiert einen Automorphismus von G. Diese Vektoren haben dieselbe Mächtigkeit wie die binär geschriebenen reellen Zahlen im Intervall $[0, 1]$ und sind damit überabzählbar.

Man kann weiter zeigen, daß G überabzählbar viele Untergruppen vom Index 2 besitzt. Andererseits ist die Anzahl der entsprechenden Fixkörper (quadratische Erweiterungen von $\mathbb{Q}$) natürlich abzählbar.

1.4 Bemerkungen

Ein Großteil der Zahlentheorie dieses Jahrhunderts kann man auffassen als Studium der absoluten Galoisgruppe $G_{\mathbb{Q}} = \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$. Die "klassische" Me-

thode, diese Gruppe in den Griff zu bekommen, besteht in der Untersuchung von Darstellungen dieser Gruppe. Dazu läßt man $G_{\mathbb{Q}}$ auf irgendwelchen K-Vektorräumen operieren, d.h. man betrachtet Homomorphismen $\phi : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_n(K)$; dabei beschränkt man sich auf stetige Homomorphismen, wobei die Gruppen $\mathrm{GL}_n(K)$ auch dann mit der diskreten Topologie versehen werden, wenn sie wie im Falle $K = \mathbb{C}$ eine natürliche Topologie tragen (das Problem ist, daß es in zusammenhängenden Gruppen wie $\mathbb{C}^\times$ zu wenig offene Untergruppen gibt). Damit ist dann $\{1\} \in \mathrm{GL}_n(K)$ offen, folglich $\ker\phi$ wegen der Stetigkeit ebenfalls offen, und damit von endlichem Index, nämlich $\ker\phi = \mathrm{Gal}\,(\overline{\mathbb{Q}}/K)$ für eine endliche normale Erweiterung $K/\mathbb{Q}$.

Betrachten wir nun eindimensionale stetige Darstellungen $\phi : G_{\mathbb{Q}} \longrightarrow \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$. Da jeder Homomorphismus einer Gruppe in eine abelsche Gruppe die Kommutatorgruppe enthält, ist $K/\mathbb{Q}$ sogar abelsch. Wegen $\mathrm{im}\,\phi \simeq G_{\mathbb{Q}}/\ker\phi$ ist $\mathrm{im}\,\phi$ endlich, und endliche Untergruppen von $\mathbb{C}^\times$ sind von Einheitswurzeln erzeugte zyklische Gruppen. Eindimensionale stetige Darstellungen von $G_{\mathbb{Q}}$ entsprechen also endlichen zyklischen Erweiterungen von $\mathbb{Q}$. Deren Studium begann mit Gauß und umfaßt Resultate wie den Dirichletschen Primzahlsatz oder den Satz von Kronecker-Weber, wonach alle abelschen Erweiterungen von $\mathbb{Q}$ in einem Kreisteilungskörper enthalten sind.

Das Studium zweidimensionaler stetiger Darstellungen begann mit Weber. Man erhält solche Objekte nämlich in natürlicher Weise, indem man $G_{\mathbb{Q}}$ auf den Torsionspunkten elliptischer Kurven operieren läßt. Eichler und Shimura haben in diesem Jahrhundert gezeigt, daß man auch gewissen Modulformen solche Darstellungen zuordnen kann, und Shimura und Taniyama haben weiter vermutet, daß die Darstellungen, welche man elliptischen Kurven über $\mathbb{Q}$ zuordnen kann, von solchen Modulformen herkommen. Insbesondere ist also der Satz von Wiles ein kleiner Schritt hin auf ein besseres Verständnis von $G_{\mathbb{Q}}$.

Geschichtliche Bemerkungen

Daß der Hauptsatz der Galoistheorie für unendliche Erweiterungen schief geht, hat bereits Dedekind [3] gesehen. Später hat E. Stiemke[2] [13] Dedekinds Idealtheorie auf unendliche Zahlkörper ausgedehnt. Emmy Noether hat sich über diese Arbeit wie folgt geäußert:

> Aller Rechnung fern, nur an den Begriffen selbst sich orientierend, mit wunderbarem Blick für das Wesentliche der Dinge – so hat dieser Zweiundzwanzigjährige eine Arbeit geschaffen, die durch die seitherige Entwicklung an keiner Stelle überholt ist.

[2] E. Stiemke, 12.04.1892 – 10.09.1915; ist im ersten Weltkrieg gefallen. Seine 1914 fertiggestellte Doktorarbeit wurde erst 1926 publiziert.

Von dieser Arbeit Stiemkes angeregt, hat sich Wolfgang Krull[3] mit diesem Thema beschäftigt, und bereits 1928 konnte er zeigen, daß der Hauptsatz der Galoistheorie bestehen bleibt, wenn man die Galoisgruppe topologisiert. Dabei berief er sich auf das Lehrbuch der Topologie von Hausdorff.[4]

Dedekinds Gegenbeispiel

Im folgenden besprechen wir Dedekinds Arbeit [3]. Wir beginnen mit einigen Erläuterungen Dedekindscher Begriffe. Sein Begriff eines "Körpers" stimmt nur insofern mit dem unseren überein, als Dedekind darunter ein "System ... von reellen oder komplexen Zahlen" versteht, also einen Teilkörper von $\mathbb{C}$. Ist L/K eine Körpererweiterung, so nennt Dedekind L ein *Multiplum* von K und K einen *Divisor* von L. Dabei bezeichnet er $\mathbb{Q}$ ("ein gemeinsame Divisor ... aller Körper") mit R und $\mathbb{C}$ ("ein gemeinsames Multiplum aller Körper") mit Z. Für den Grad der Erweiterung L/K schreibt Dedekind (L, K), und er erwähnt die Formel $(M : K) = (M : L)(L : K)$ für Türme $M/L/K$.

Als *Permutation* von L bezeichnet Dedekind eine Abbildung $L \longrightarrow \mathbb{C}$ mit folgenden Eigenschaften:

- $(u + v)\phi = u\phi + v\phi$;
- $(u - v)\phi = u\phi - v\phi$;
- $(uv)\phi = (u\phi)(v\phi)$;
- $\frac{u}{v}\phi = \frac{u\phi}{v\phi}$.

Man beachte, daß Dedekind seine Automorphismen von rechts operieren läßt. Weiter bemerkt er, daß mit K auch K^ϕ ein Körper ist und daß die rationalen Zahlen von ϕ festgelassen werden.

Ist L/K eine Erweiterung und operiert ϕ auf L, so heißt die Einschränkung ψ von ϕ auf K *der Divisor* von ϕ, während ϕ *ein Multiplum* von ψ heißt. Ist $\mathfrak{P}$ ein System von Permutationen auf L und hat ein $t \in L$ genau n verschiedene Bilder, so heißt t eine bezüglich $\mathfrak{P}$ n-wertige Zahl. Dedekinds erster, "leicht zu beweisender Satz" besagt

Satz 1.14. *Ist $\mathfrak{P}$ ein System von Körper-Permutationen ψ, so bildet die Gesamtheit aller zu $\mathfrak{P}$ einwertigen Zahlen einen Körper A; die Permutationen ψ haben alle einen und denselben auf A bezüglichen Divisor ϕ, und jeder gemeinsame Divisor der Permutationen ψ ist Divisor dieser Permutation ϕ.*

[3] W. Krull, 26.08.1899 (Baden-Baden) – 12.04.1971 (Bonn).

[4] Felix Hausdorff, 8.11.1869 (Breslau) – 26.01.1942 (Bonn). Hausdorff promovierte in Leipzig und arbeitete ab 1910 in Bonn. 1935 wurde er von den Nazis entlassen, und als 1942 die Einweisung in ein Lager bevorstand, beging er mit seiner Frau und deren Schwester Selbstmord.

Dedekind nennt A den Körper von $\mathfrak{P}$, in heutiger Nomenklatur ist das der Fixkörper des Systems $\mathfrak{P}$. Sein zweiter Satz behandelt das Liften von Automorphismen:

Satz 1.15. *Ist der Körper B ein endliches Multiplum des Körpers A und ϕ eine Permutation von A, so ist der Grad (B, A) auch die Anzahl aller verschiedenen Permutationen ψ von B, welche Multipla von ϕ sind; zugleich ist A der Körper, und ϕ der Rest des Systems $\mathfrak{P}$ dieser Permutationen.*

Springen wir jetzt in den letzten Paragraphen; er beginnt so:

> Wir haben gesehen, daß der aus allen algebraischen Zahlen bestehende Körper H unendlich viele Permutationen ω besitzt, und daß er durch jede von ihnen in sich selbst übergeht; diese Permutationen ω bilden daher eine unendliche Gruppe, die wir mit $\mathfrak{G}$ bezeichnen wollen, und wir fragen, ob wohl auch hier eine gegenseitig eindeutige Korrespondenz zwischen den algebraischen Körpern A (den Divisoren von H) und den in $\mathfrak{G}$ enthaltenen Gruppen $\mathfrak{A}$ besteht.

Etwas später schreibt er

> ... aber es fehlt der Nachweis, daß ... die Körper zweier verschiedener Gruppen auch verschieden sind. Dies habe ich anfangs für sehr wahrscheinlich gehalten, und erst nach mehreren vergeblichen Versuchen, es zu beweisen, ist es mir gelungen, mich von der Unrichtigkeit dieser Vermutung durch ein Beispiel zu überzeugen, welches ich zum Schluß dieser Arbeit jetzt noch mitteilen will.

Im folgenden sollen Dedekinds Argumente in moderner Notation nachvollzogen werden. Sei p eine feste Primzahl, $K_n = \mathbb{Q}(\zeta_{p^n})$ der Körper der p^n-ten Einheitswurzeln, und $L = \bigcup_{n\geq 1} K_n$. Jeder Automorphismus ε von $L/\mathbb{Q}$ induziert via Restriktion einen Automorphismus ε_n von K_n, und die Kette $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ hat die Eigenschaft, daß jedes ε_n die Einschränkung *jedes* ε_{n+s} für $s \geq 0$ ist. Ist umgekehrt eine Kette von Automorphismen mit dieser Eigenschaft gegeben, so existiert ein Automorphismus ε von L, dessen Einschränkung auf K_n gerade ε_n ergibt:

Nun ist ein ε_n vollständig bestimmt durch die Angabe eines $u_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ mit $\zeta_{p^n}^{\varepsilon_n} = \zeta_{p^n}^{u_n}$. Setzen wir $(n, \varepsilon) = u_n$. Aus $\zeta_{p^n}^{\varepsilon} = (\zeta_{p^{n+1}}^{\varepsilon})^p$ folgt dann $(n, \varepsilon) \equiv (n+1, \varepsilon) \bmod p^n$. Jeder Automorphismus ε definiert uns also eine Folge von Zahlen $(n, \varepsilon) \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ mit der Verträglichkeitseigenschaft $(n, \varepsilon) \equiv (n + s, \varepsilon) \bmod p^n$ für alle $s \geq 0$. Schreiben wir (n, ε) in der Form $(n, \varepsilon) = a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1}$, so bedeutet die Verträglichkeit, daß die Entwicklung von $(n+s, \varepsilon)$ genauso beginnt. Ist Umgekehrt eine verträgliche Folge solcher Zahlen gegeben, wird dadurch ein $\varepsilon \in \mathrm{Gal}(L/\mathbb{Q})$ definiert. Mit anderen Worten: es gibt eine Bijektion zwischen den Automorphismen von $L/\mathbb{Q}$ und den p-adischen

Zahlen $\mathbb{Z}_p^\times$, wobei die Operation von $a = a_0 + a_1 p + a_2 p^2 + \ldots$ auf ζ_{p^n} durch $\zeta_{p^n} \longmapsto \zeta_{p^n}^\alpha$ mit $\alpha \equiv a \bmod p^n$ definiert ist.

Dedekind kennt die p-adischen Zahlen anscheinend nicht (sie wurden 1897 von Hensel entdeckt, aber erst um 1920 herum hinreichend bekannt). Nachdem er im wesentlichen $\mathrm{Gal}\,(L/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ gezeigt hat, fragt er nach den endlichen Untergruppen von $\mathbb{Z}_p^\times$ und findet, daß es für $p \neq 2$ genau $p-1$ Automorphismen endlicher Ordnung gibt. Wir schreiben das heute in der Form $\mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$, wobei $\mathbb{Z}/(p-1)\mathbb{Z}$ die Untergruppe der in $\mathbb{Z}_p$ enthaltenen Einheitswurzeln ist.

Dedekind macht das so: er setzt $(1, \varepsilon) = a$ für ein $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ (das sind genau $p-1$ Möglichkeiten) und setzt $(n, \varepsilon) \equiv (1, \varepsilon)^{p^{n-1}} \bmod p^n$. Wegen der Verträglichkeit ist damit ein Automorphismus ε von L/K definiert, der per Konstruktion $\varepsilon^{p-1} = 1$ genügt (Dedekind konstruiert hier natürlich den p-adischen Grenzwert $\alpha = \lim a^{p^n}$ in $\mathbb{Z}_p$).

Nun sei g eine Primitivwurzel modulo p^2 und damit modulo p^n für alle $n \geq 1$. Sei β derjenige Automorphismus von $L/\mathbb{Q}$, welcher ζ_{p^n} auf $\zeta_{p^n}^g$ abbildet, und sei H die von β algebraisch erzeugte Gruppe. Dann ist $\mathbb{Q}$ der Fixkörper von H, da β jedes endliche $\mathrm{Gal}\,(K_n/\mathbb{Q})$ erzeugt; andererseits kann H nicht gleich der ganzen Galoisgruppe sein, da beispielsweise H keine endlichen Elemente enthält und $G \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ ist.

Abschließend noch ein Zitat Dedekinds aus seinem Brief an Frobenius vom 18. April 1897:

> Für die unendlichen Körper hat bisher ein "Noli me tangere"[5] gegolten; nur deshalb möchte ich gern einmal von ihnen sprechen.

Literatur

Wenn man Bücher über Galoistheorie empfiehlt, sollte man den Namen Emil Artin nicht vergessen. Zwar enthält der Klassiker [1] nur die endliche Version, dafür ist die Galoistheorie unendlicher Erweiterungen in [2] so gut, daß Moreno [12] daraus abgeschrieben hat. Das Dover-Buch von McCarthy [10] ist nicht schlecht (in seiner schwäbischen Bedeutung) und recht billig (das kommt der schwäbischen Sparsamkeit ebenfalls entgegen). Das Lehrbuch von Morandi ist eine empfehlenswerte moderne Quelle. Der Übersichtsartikel von Jarden [6] schließlich zeigt, wo die Reise hingeht.

Einführungen in das Gebiet topologischer Gruppen bieten Lutz [9] und Higgins [5].

1. E. Artin, *Galoissche Theorie*, Harri Deutsch 1988

2. E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach 1967

[5] "Rühr mich nicht an".

3. R. Dedekind, *Über die Permutationen des Körpers aller algebraischen Zahlen*, Festschrift Gött. Ges. Wiss., Berlin 1901; Ges. Werke, ??

4. F. Hausdorff, *Mengenlehre*, Leipzig 1914, 3. Aufl. 1935; jüngste Auflage 1991 in englischer Übersetzung

5. P.F. Higgins, *Topological Groups*, London Math. Soc. 1974

6. M. Jarden, *Infinite Galois theory*, in: Handbook of algebra, Vol. 1, 269–319, North-Holland, Amsterdam, 1996

7. W. Krull, *Galoissche Theorie der unendlichen algebraischen Erweiterungen*, Math. Ann. **100** (1928), 687–698

8. F. Lorenz, *Einführung in die Algebra I*, Spektrum 1997

9. D. Lutz, *Topologische Gruppen*, B.I. 1976

10. P.J. McCarthy, *Algebraic Extensions of Fields*, Dover 1976

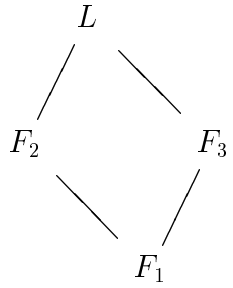
11. P. Morandi, *Field and Galois theory*, Graduate Texts in Mathematics, 167. Springer-Verlag, New York, 1996

12. C.J. Moreno, *Advanced analytic number theory. I: Ramification theoretic methods*, Contemp. Math. 15, 190 p. (1983)

13. E. Stiemke, Math. Z. **25** (1926), 9–39

Kapitel 2
Projektive Limites

2.1 Galoisgruppen



Sei L/K eine unendliche Galoiserweiterung. Dann ist $L = \bigcup F$ die Vereinigung von endlichen normalen Teilerweiterungen F/K. Zu jedem solchen System haben wir natürliche Homomorphismen $\pi_F : \mathrm{Gal}\,(L/K) \longrightarrow \mathrm{Gal}\,(F/K)$, nämlich die Restriktionen. Sind F_j/K $(j = 1, 2, 3)$ Teilerweiterungen mit $F_1 \subseteq F_2 \cap F_3$, dann sind die Homomorphismen $\pi_j : \mathrm{Gal}\,(L/K) \longrightarrow \mathrm{Gal}\,(F_j/K)$ kompatibel in dem Sinne, daß $\pi_1 = \pi_{2,1} \circ \pi_2 = \pi_{3,1} \circ \pi_3$ ist, wobei $\pi_{j,1}$ die Restriktion $\mathrm{Gal}\,(L/F_1) \longrightarrow \mathrm{Gal}\,(F_j/F_1)$ bezeichnet. Diese Situation läßt sich nun so formalisieren, daß unendliche Galoisgruppen ebenso wie beispielsweise die p-adischen Zahlen $\mathbb{Z}_p$ erfaßt werden.

Dazu nennen wir eine partiell geordnete Indexmenge I *gerichtet*, wenn es zu allen $i, j \in I$ ein $k \in I$ gibt mit $i \leq k$ und $j \leq k$. Zu jedem Index $i \in I$ sei nun eine Gruppe G_i gegeben, und zu jedem Indexpaar mit $i \leq j$ ein Gruppenhomomorphismus $\pi_{ji} : G_j \longrightarrow G_i$ mit der Eigenschaft, daß π_{ii} die Identität ist und weiter $\pi_{ji} \circ \pi_{kj} = \pi_{ki}$ für alle $i \leq j \leq k$ gilt. Ein solches System $(I, \leq, \{G_i\}, \pi_{ji})$ heißt *projektives System* von Gruppen.

Jedem solchen projektiven System kann man eine Untergruppe des direkten Produktes $G = \prod G_i$ zuordnen, nämlich die Teilmenge der "verträglichen" Elemente: wir setzen

$$\varprojlim G_i = \{(\ldots, g_i, \ldots) \in G : \pi_{kj}(g_k) = g_j, \text{ falls } i \leq k\}.$$

Dies ist in der Tat eine Untergruppe: zum einen ist das System $(1,1,1,\dots)$ verträglich, also Element (und zwar neutrales) von $\varprojlim G_i$ (insbesondere ist $\varprojlim G_i$ nie leer), zum andern ist mit $g=(\dots,g_i,\dots)\in\varprojlim G_i$ und $h=(\dots,h_i,\dots)\in\varprojlim G_i$ auch $gh=(\dots,g_ih_i,\dots)\in\varprojlim G_i$. Dazu ist nachzurechnen, daß gh wirklich verträglich ist. Wegen $\pi_{kj}(g_kh_k)=\pi_{kj}(g_k)\pi_{kj}(h_k)=g_jh_j$ ist das aber in Ordnung.

Die Gruppe $\varprojlim G_i$ nennt man den projektiven (oder auch inversen) Limes des Systems $(I,\leq,\{G_i\},\pi_{ji})$. Neben der Gruppe $\varprojlim G_i$ erhält man als Zugabe noch Projektionen $\pi_j:\varprojlim G_i\longrightarrow G_j$, die durch die Projektionen $\prod G_i\longrightarrow G_j$ induziert werden.

Setzen wir nun voraus, daß alle G_i kompakte hausdorffsche topologische Gruppen sind (z.B. endliche Gruppen mit der diskreten Topologie), so ist das Produkt $\prod G_i$ mit der Produkttopologie (die gröbste Topologie, in der die Projektionen π_j stetig sind) nach dem Satz von Tychonoff ebenfalls kompakt. Wenn wir zeigen können, daß $\varprojlim G_i$ abgeschlossen in $\prod G_i$ ist, folgt, daß $\varprojlim G_i$ eine kompakte topologische Gruppe ist. Das geht in der Tat:

Proposition 2.1. *Ist jedes G_i hausdorffsch, und sind die Homomorphismen π_{ji} stetig, dann ist $\varprojlim G_i$ abgeschlossen in $G=\prod G_i$ (bezüglich der Relativtopologie).*

Beweis. Sei $g=(\dots,g_i,\dots)\in G\setminus\varprojlim G_i$, so gibt es ein Paar (i,f) mit $j\geq i$ und $\pi_{ji}(g_j)\neq g_i$. Da die G_i hausdorffsch sind, gibt es offene Umgebungen U_j' von $\pi_{ji}(g_j)\in G_i$ und U_i von $g_i\in G_i$ mit $U_j'\cap U_i=\varnothing$. Da π_{ji} stetig ist, ist $U_j=\pi_{ji}^{-1}(U_j')$ eine offene Umgebung von $g_j\in G_j$. Dann ist

$$U=U_i\times U_j\times\prod_{k\neq i,j}G_k$$

eine offene Umgebung von $g\in G$. Nun ist aber $U\cap\varprojlim G_i=\varnothing$, denn nach Konstruktion haben $\pi_{ji}(U_j)\subset U_j'$ und U_i leeren Schnitt. Jedes $g\in G\setminus\varprojlim G_i$ besitzt folglich eine Umgebung, die $\varprojlim G_i$ nicht schneidet. Also ist $G\setminus\varprojlim G_i$ offen und damit $\varprojlim G_i$ abgeschlossen. □

Projektive Limites endlicher diskreter Gruppen nennen wir pro-endliche Gruppen. Da alle G_i endlich mit der diskreten Topologie, also kompakt, hausdorffsch und total unzusammenhängend sind, gilt dies auch für das direkte Produkt (nur die Kompaktheit, die von Tychonoff garantiert wird, ist schwierig), und damit wegen der Abgeschlossenheit von $\varprojlim G_i$ in $\prod G_i$ auch für die pro-endliche Gruppe $\varprojlim G_i$. Damit haben wir das

Korollar 2.2. *Pro-endliche Gruppen sind kompakte hausdorffsche und total unzusammenhängende topologische Gruppen.*

Bemerkung. Die Umkehrung gilt übrigens auch: Pro-endliche Gruppen lassen sich also topologisch charakterisieren.

Wir bemerken außerdem, daß die zu $G = \varprojlim G_i$ gehörigen Projektionen $\pi_i : G \longrightarrow G_i$ automatisch stetig sind, wenn das für die π_{ji} gilt (insbesondere also im Falle pro-endlicher Gruppen).

Die Standardbeispiele pro-endlicher Gruppen sind:

- endliche Gruppen: ist G endlich, so definiert $(I, \leq, G_i, \pi_{ji})$ mit $I = \{1\}$, $G_i = G$ und $\pi_{11} = \mathrm{id}$ ein projektives System mit Limes G.
- Galoisgruppen: Sei L/K eine galoissche Erweiterung; durchläuft F/K die endlichen normalen Teilerweiterungen, so bilden die Galoisgruppen $\mathrm{Gal}\,(F/K)$ zusammen mit den Restriktionen ein projektives System. Insbesondere ist $G = \varprojlim \mathrm{Gal}\,(F/K)$ eine pro-endliche Gruppe. Tatsächlich gilt $G = \mathrm{Gal}\,(L/K)$: denn jeder Automorphismus $\phi \in \mathrm{Gal}\,(L/K)$ definiert auf offensichtliche Weise ein verträgliches System und ist damit in G enthalten, umgekehrt kann man jedes verträgliche System als Automorphismus von L/K auffassen.
- Die p-adischen Zahlen $\mathbb{Z}_p$: Sei $G_n = \mathbb{Z}/p^n\mathbb{Z}$ und $\pi_{mn} : \mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ die natürliche Projektion. Dann ist $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ der Ring der ganzen p-adischen Zahlen (projektive Limites von Ringen bilden wieder einen Ring). Die pro-endliche Konstruktion der $p-1$ Einheitswurzeln in $\mathbb{Z}_p$ verläuft wie folgt: sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$; dann ist $(a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z}$ mit $a_n = a^{p^n} + p^{n+1}\mathbb{Z}$ ein verträgliches System: dazu ist nur zu zeigen, daß $a^{p^m} \equiv a^{p^n} \bmod p^{n+1}$ gilt für alle $m \geq n$. Aber nach Division durch a^{p^n} ist dies gleichbedeutend mit $1 \equiv a^{p^m - p^n} \bmod p^{n+1}$, und da $p^m - p^n = p^n(p^{m-n} - 1)$ durch $p^n(p-1) = \phi(p^{n+1})$ teilbar ist, ist dies in der Tat richtig. Ist $\overline{a}$ das dadurch definierte Element von $\mathbb{Z}_p$, so folgt $\overline{a}^{p-1} = 1$, weil dies auf jedem endlichen Niveau richtig ist.

Bei diesen Beispielen ist natürlich noch nachzuweisen, daß die pro-endliche Topologie mit der Krullschen bzw. von der p-adischen Metrik induzierten Topologie übereinstimmt. Dazu benutzen wir folgenden

Hilfssatz 2.3. *Sei* $(I, \leq, \{G_i\}, \pi_{ji})$[1] *ein projektives System endlicher Gruppen und* $G = \varprojlim G_i$ *die dadurch definierte pro-endliche Gruppe. Dann bilden die Mengen* $\{\ker (G \longrightarrow G_i) : I \in I\}$ *eine offene Umgebungsbasis der* 1 *in* G.

[1] Künftig werden wir das etwas schlampiger in der Form (G_i, π_{ji}) schreiben. Man beachte auch, daß für eine endliche Gruppe G gilt $\varprojlim G_i = G$, wenn $G_i = G$ und $\pi_{ji} = \mathrm{id}$ ist, dagegen $\varprojlim G_i = 0$, wenn man für die π_{ji} die Nullabbildungen wählt.

Beweis. Da die G_i endlich und mit der diskreten Topologie versehen sind, ist $\{1\}$ eine offene Umgebungsbasis der 1 in G_i. Nach Definition der Produkttopologie von $\prod G_i$ (fast überall alles, an endlich vielen Stellen etwas offenes) und der Relativtopologie von $G \subseteq \prod G_i$ bilden die Mengen

$$G \cap \Big(\prod_{j \in J} \{1\} \times \prod_{i \in I \setminus J} G_i \Big)$$

eine Umgebungsbasis der 1 in G; hierbei durchläuft J die endlichen Teilmengen von I. Nun ist aber

$$G \cap \Big(\prod_{j \in J} \{1\} \times \prod_{i \in I \setminus J} G_i \Big) = \bigcap_{J \subseteq I} \ker (G \longrightarrow G_i),$$

und die Behauptung folgt jetzt aus der Beobachtung, daß es wegen der Endlichkeit von J und der Tatsache, daß I gerichtet ist, ein $k \in I$ gibt mit $j \leq k$ für alle $j \in J$: damit ist nämlich

$$\ker (G \longrightarrow G_k) \ \subseteq \ \bigcap_{J \subseteq I} \ker (G \longrightarrow G_i),$$

d.h. die Kerne der Projektionen π_i bilden in der Tat eine offene Umgebungsbasis der 1 in G. □

Damit ist es ein Leichtes, die pro-endliche und die Krull-Topologie von $G = \mathrm{Gal}\,(L/K)$ zu identifizieren: eine offene Umgebungsbasis der 1 in der Krulltopologie von G besteht aus den Gruppen $G_i = \mathrm{Gal}\,(F_i/K)$, wobei F_i/K endlich und normal ist. Andererseits ist $G = \varprojlim G_i$, und $\ker (G \longrightarrow G_i)$ besteht aus allen Automorphismen, deren Einschränkung auf F_i trivial ist, d.h. es ist $\ker (G \longrightarrow G_i) = \mathrm{Gal}\,(L/F_i)$.

Genauso einfach ist es, die Topologie der p-adischen Zahlen mit der pro-endlichen Topologie von $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ zu identifizieren: bekanntlich bilden die Gruppen $p^n\mathbb{Z}_p$ eine offene Umgebungsbasis der $1 \in \mathbb{Z}_p$; auf der andern Seite ist offenbar $\ker (\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}) = p^n\mathbb{Z}_p$.

Ist (R_i, π_{ji}) ein projektives System von Ringen (alle Ringe mit 1, die π_{ji} Ringhomomorphismen, also $\pi_{ji}(1) = 1$), dann ist auch $R = \varprojlim R_i$ ein Ring mit 1, und es gilt $R^\times = \varprojlim R_i^\times$. Insbesondere ist $\mathbb{Z}_p^\times = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \varprojlim \mathbb{Z}/(p-1)\mathbb{Z} \times (\mathbb{Z}/p^{n-1}\mathbb{Z})^\times$. Nun ist das Bilden des projektiven Limes mit dem direkten Produkt (von Gruppen, Ringen, ...) verträglich, somit $\mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. Dabei haben wir $\varprojlim \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ verwendet, und das müssen wir noch begründen.

Ist nämlich G irgendeine endliche Gruppe, und setzen wir $I = \mathbb{N}$, $G_i = G$ und $\pi_{ji} = 0$, so ist $\varprojlim G_i = 0$. Im obigen Beispiel ist also nachzuweisen, daß die von $\pi_{mn} : (\mathbb{Z}/p^m\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$ induzierte Abbildung $\rho_{mn} : \mathbb{Z}/(p-1)\mathbb{Z} \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}$ die Identität ist. Das ist aber klar, sobald man aufschreibt, was passiert.

2.2 Funktorielle Eigenschaften des projektiven Limes

Eine Teilmenge $J \subseteq I$ einer gerichteten Menge I heißt cofinal, wenn es zu jedem $i \in I$ ein $j \in J$ mit $i \leq j$ gibt. Man überzeugt sich leicht davon, daß mit $(I, \leq, G_i, \pi_{i'i})$ auch $(J, \leq, G_j, \pi_{j'j})$ ein projektives System ist, und daß $\varprojlim G_i = \varprojlim G_j$ gilt.

Der Punkt, der uns als nächstes beschäftigen wird, kann etwas salopp mit "projektive Limites von Surjektionen sind surjektiv" beschrieben werden – mit der Einschränkung im Hinterkopf, daß das nur für projektive Systeme kompakter Räume gilt, insbesondere also im pro-endlichen Fall. Beim Beweis dieser Tatsache sind schon ganz andere als ich zu Hochform aufgelaufen:

- Moreno: the surjectivity of the π_{ji} implies the surjectivity of π_i;
- Ribes [p. 36]: verweist auf B_3, §9, Prop. 8;
- Koch: verweist auf Pontrjagin;
- Poitou [3]: auf die Lücke in seinem Beweis gehen wir noch genauer ein.

Nun zum Beweis: der wesentliche Punkt ist die Behauptung, daß die zu beweisende Aussage in der Kategorie der Mengen richtig ist. Das Problem ist nämlich, daß die Urbilder von Elementen (man muß ja zeigen, daß diese im Limes nicht leer sind) keine Gruppen sind und man so automatisch aus der Kategorie endlicher Gruppen herausfällt.

Proposition 2.4. *Sei (X_i, π_{ji}) ein projektives System nichtleerer hausdorffscher topologischer Räume. Sind die π_{ji} alle surjektiv und ist das Urbild jedes Punktes kompakt, dann sind die Projektionen $\pi_i : \varprojlim X_i \longrightarrow X_i$ ebenfalls surjektiv, und insbesondere ist $\varprojlim X_i \neq \varnothing$.*

Beweis. Da die Menge $J = \{j \in I : j \geq i\}$ cofinal in I ist, dürfen wir I durch J ersetzen. Sei ein $x_i \in X_i$ gegeben; wegen der Surjektivität der π_{ji} gibt es für alle $j \in J$ ein x_j mit $\pi_{ji}(x_j) = x_i$, und damit ist dann $(\dots, x_j, \dots) \in \prod_{j \in J} \pi_{ji}^{-1}(x_i) =: Y$. Da die Urbilder von Punkten nach Voraussetzung kompakt ist, ist Y nach Tychonoff ebenfalls kompakt. Für jedes Paar $(j,k) \in J \times J$ mit $j \leq k$ betrachten wir nun die Teilmenge $F_{jk} = \{(\dots, x_j, \dots) \in Y : x_j = \pi_{jk}(x_k)\}$ von Y. Dann ist jedes F_{jk} abgeschlossen, und jeder endliche Durchschnitt solcher Mengen ist nicht leer: wir brauchen ja nur einen Index $n \in J$ zu nehmen, der größer ist als diejenigen, die in den Indizes der endlich vielen F_{jk} auftauchen, wählen ein x_n und definieren $x_k = \pi_{nk}(x_n)$ für alle $k \leq n$. Wegen der Kompaktheit von Y sind dann auch beliebige Durchschnitte nicht leer, insbesondere gibt es ein x, welches im Durchschnitt aller F_{jk}, also in $\varprojlim X_i$ liegt. Damit ist dann $\pi_i(x) = x_i$. □

Diese Surjektivität ist uns bereits im letzten Kapitel begegnet: betrachte eine unendliche Galoiserweiterung L/K und schreibe $\mathrm{Gal}\,(L/K) = \varprojlim \mathrm{Gal}\,(F/K)$, wo F/K die endlichen normalen Teilerweiterungen durchläuft. Die zu solchen endlichen Erweiterungen $F_1 \subset F_2 \subset L$ gehörigen Projektionen $\mathrm{Gal}\,(F_2/K) \longrightarrow \mathrm{Gal}\,(F_1/K)$ sind nach der endlichen Galoistheorie alle surjektiv; Proposition 2.4 besagt, daß auch die Restriktionen $\mathrm{Gal}\,(L/K) \longrightarrow \mathrm{Gal}\,(F/K)$ surjektiv sind, d.h. daß man jeden Automorphismus von F/K zu einem solchen von L/K liften kann. Das Auswahlaxiom, das wir in Kapitel 1 benutzt haben, ist hier natürlich im Satz von Tychonoff versteckt.

Manchmal[2] werden pro-endliche Gruppen definiert als projektive Limites endlicher Gruppen G_i, bei denen die Homomorphismen π_{ji} sämtlich surjektiv sind. Das folgende Resultat scheint zu zeigen, daß dies keine Einschränkung ist:

Lemma 2.5. *Sei $(I, \leq, \{G_i\}, \pi_{ji})$ projektives System endlicher Gruppen. Dann existiert ein projektives System $(I, \leq, \{H_i\}, \rho_{ji})$ mit $\varprojlim G_i \simeq \varprojlim H_i$ derart, daß alle ρ_{ji} surjektiv sind. Insbesondere sind die Projektionen $\rho_j : \varprojlim H_i \longrightarrow H_i$ surjektiv.*

Beweis. Sei $H_i = \bigcap_{k \geq i} \mathrm{im}\,\pi_{ki}$; dann ist $H_i \subseteq G_i$, und die Einschränkung von $\pi_{ji} : G_j \longrightarrow G_i$ definiert einen surjektiven Homomorphismus $\rho_{ji} : H_j \longrightarrow H_i$ (man muß nachrechnen, daß ρ_{ji} in H_i landet und surjektiv ist; beides ist mehr oder weniger offensichtlich). Ebenso leicht überzeugt man sich davon, daß $\varprojlim G_i \simeq \varprojlim H_i$ gilt (algebraisch): das liegt daran, daß mit $(\dots, g_i, \dots) \in \varprojlim G_i$ automatisch jedes $g_i \in H_i$ liegt. Bleibt noch, die Topologien zu vergleichen: es ist aber $\ker(G \longrightarrow G_i) = \ker(H \longrightarrow H_i)$ wegen $\pi_{ji} = \iota \circ \rho_{ji}$, wo $\iota : H_i \longrightarrow G_i$ die Einbettung von H_i in G_i ist. Die letzte Behauptung folgt aus Proposition 2.4. □

Nun wieder zurück zur Frage der Surjektivität.

Proposition 2.6. *Sei F ein kompakter hausdorffscher Raum und (ϕ_i) ein Morphismus des projektiven Systems $(F, 1)$ in das projektive System (G_i, π_{ji}) von hausdorffschen Räumen derart, daß die induzierte Abbildung $\phi : F \longrightarrow \varprojlim G_i$ stetig ist. Sind dann alle ϕ_i surjektiv, so auch ϕ.*

Beweis. Sei $g = (g_i) \in G = \varprojlim G_i$ und $K_i := \phi_i^{-1}(g_i)$. Ist $i \leq j$, so gilt $K_i \supseteq K_j$: also ist jeder endliche Durchschnitt der K_i nicht leer. Wegen der Kompaktheit von F enthält dann der Durchschnitt über alle K_i ein $f \in F$, und damit ist $\phi_i(f) = g_i$, folglich $\phi(f) = g$. □

[2] Z.B. im Buch von Moreno (sh. Kapitel 1).

Satz 2.7. *Seien (G_i, π_{ji}) und (H_i, ρ_{ji}) projektive Systeme von Gruppen, und seien G bzw. H die entsprechenden pro-endlichen Gruppen; für jedes $i \in I$ möge ein Homomorphismus $\phi_i : G_i \longrightarrow H_i$ existieren, welcher mit den π_{ji} und den ρ_{ji} verträglich ist, d.h. für welchen*

$$\begin{array}{ccc} G_j & \xrightarrow{\pi_{ji}} & G_i \\ {\scriptstyle\phi_j}\downarrow & & \downarrow{\scriptstyle\phi_i} \\ H_j & \xrightarrow{\rho_{ji}} & H_i \end{array} \tag{2.1}$$

kommutiert. Dann induziert das System $\{\phi_i\}$ einen Homomorphismus $\phi : G \longrightarrow H$, für den das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\pi_i} & G_i \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_i} \\ H & \xrightarrow{\rho_i} & H_i \end{array} \tag{2.2}$$

kommutiert. Sind alle ϕ_i injektiv, dann auch ϕ.

Sind darüberhinaus alle G_i und H_i kompakt und die Homomorphismen π_{ji}, ρ_{ji} und ϕ_i stetig (z.B. im Falle endlicher diskreter Gruppen), so ist ϕ stetig; sind weiter alle ϕ_i surjektiv, so auch ϕ.

Insbesondere ist also der projektive Limes stetiger surjektiver Abbildungen zwischen kompakten hausdorffschen Räumen wieder surjektiv.

Beweis. Sei $g = (\dots, g_i, \dots) \in G$. Wir können jedes g_i mit ϕ_i auf ein $h_i \in H_i$ abbilden und $\phi(g) = h := (\dots, h_i, \dots) \in \prod H_i$ setzen. Damit gilt dann

- $h \in H$: für $i \leq j$ ist nämlich $\rho_{ji}(h_j) = \rho_{ji} \circ \phi_j(g_j)$, und die Kommutativität von (2.1) gibt $\rho_{ji} \circ \phi_j(g_j) = \phi_i \circ \pi_{ji}(g_j) = \phi_i(g_i) = h_i$. Also bilden die h_i ein verträgliches System, und es ist $h \in H$.
- $\phi(g'g) = \phi(g)\phi(g')$: dies ist klar, da die ϕ_i Homomorphismen sind.
- Das Diagramm (2.2) kommutiert: ist $h = \phi(g)$ und $h_i = \rho_i(h)$, so ist $h_i = \pi_i(g_i)$ nach Definition von ϕ, und $g_i = \pi_i(g)$.

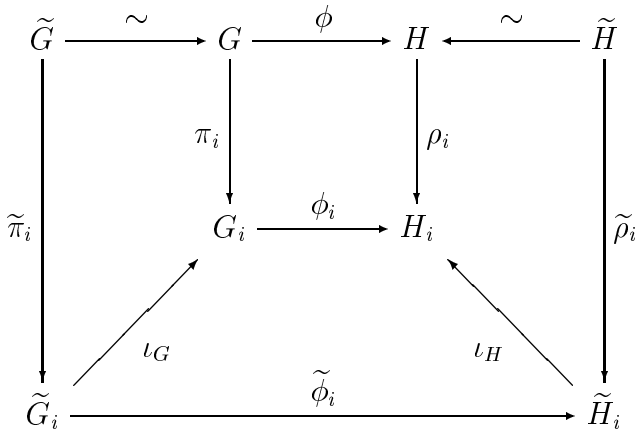
Seien nun die ϕ_i injektiv und $\phi(g) = 1$. Dann ist $h_i = 1$ für alle $i \in I$, und wegen $\phi_i(g_i) = h_i = 1$ folgt $g_i = 1$ für alle $i \in I$, also $g = 1$.

Nun zur Surjektivität. Nehmen wir zuerst an, die π_{ji} seien surjektiv. Dann sind nach Proposition 2.4 die Projektionen π_i surjektiv, somit auch die Abbildungen $\phi_i \circ \pi_i : G = \varprojlim G_i \longrightarrow H_i$. Nach Proposition 2.6 ist dann auch der davon induzierte Homomorphismus $G \longrightarrow H = \varprojlim H_i$ surjektiv.

Soweit der Beweis von Poitou [3] im Falle, daß alle π_{ji} surjektiv sind. Der allgemeine Beweis wird mit der Bemerkung abgetan, man könne die G_i durch

die $\widetilde{G}_i = \cap \operatorname{im} \pi_{ji}$ ersetzen. Das kann man in der Tat, nur sind dann die Einschränkungen der ϕ_i auf $\widetilde{G}_i \longrightarrow H_i$ im allgemeinen nicht mehr surjektiv, und der Beweis geht nicht mehr durch. In der Tat muß man hier etwas mehr tun.

Wir haben verträgliche Abbildungen $\sigma_j = \phi_j \circ \pi_j : G \longrightarrow H_i$. Wir ersetzen die projektiven Systeme (G_i, π_{ji}) und (H_i, ρ_{ji}) mit Lemma 2.5 durch $(tG_i, \widetilde{\pi}_{ji})$ $(\widetilde{H}_i, \widetilde{\rho}_{ji})$, wobei die $\widetilde{\rho}_{ji}$ surjektiv sind. Wir behaupten, daß wir durch Einschränken von $\phi_i : G_i \longrightarrow H_i$ einen surjektiven Homomorphismus $\widetilde{\phi}_j : \widetilde{G}_i \longrightarrow \widetilde{H}_i$ erhalten.



Dazu ist erst einmal zu zeigen, daß $\widetilde{\phi}_i$ in $\widetilde{H}_i$ landet. Nach Definition der $\widetilde{G}_i$ existiert zu jedem $g_i \in \widetilde{G}_i$ für jedes $k \geq i$ ein $g_k \in G_k$ mit $g_i = \pi_{ki}(g_k)$. Also folgt $\phi_i(g_i) = \phi_i \circ \pi_{ki}(g_k) = \rho_{ki} \circ \phi_k(g_k) \in \operatorname{im} \rho_{ki}$, und wir sehen im $\phi_i \subseteq \widetilde{H}_i$.

Weiter ist nachzuweisen, daß $\widetilde{\phi}_i$ surjektiv ist. Sei also $h_i \in \widetilde{H}_i$. Dann ist $h_i = \widetilde{\rho}_{ji}(h_j)$, wegen der Surjektivität von ϕ_j ist $h_j = \phi_j(g_j)$ für ein g_j, somit $h_i = \widetilde{\rho}_{ji} \circ \phi_j(g_j) = \phi_i(\pi_{ji}(g_j))$. Also ist $h_i \in \phi_i(\bigcap \operatorname{im} \pi_{ji}) = \phi_i(\widetilde{G}_i)$, und das war zu zeigen.

Wenden wir das bereits bewiesene auf die Systeme $\widetilde{G}_i$ und $\widetilde{H}_i$ an, so folgt die Behauptung im allgemeinen Fall. □

Seien (A_i, π_{ji}), (B_i, ρ_{ji}) und (C_i, σ_{ji}) projektive Systeme endlicher Gruppen; wir sagen, das System von Sequenzen

$$1 \longrightarrow (A_i) \longrightarrow (B_i) \longrightarrow (C_i) \longrightarrow 1$$

sei exakt, wenn für jedes $i \in I$ die Sequenz

$$1 \longrightarrow A_i \longrightarrow B_i \longrightarrow C_i \longrightarrow 1$$

exakt ist, und wenn die Diagramme

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A_j & \longrightarrow & B_j & \longrightarrow & C_j & \longrightarrow & 1 \\ & & {\scriptstyle \pi_{ji}}\downarrow & & {\scriptstyle \rho_{ji}}\downarrow & & {\scriptstyle \sigma_{ji}}\downarrow & & \\ 1 & \longrightarrow & A_i & \longrightarrow & B_i & \longrightarrow & C_i & \longrightarrow & 1 \end{array}$$

für alle Paare $i, j \in I$ mit $i \leq j$ kommutieren. Damit haben wir

Satz 2.8. *Sei*

$$1 \longrightarrow (A_i) \xrightarrow{\alpha_i} (B_i) \xrightarrow{\beta_i} (C_i) \longrightarrow 1$$

ein exaktes projektives System endlicher Gruppen; dann ist auch

$$1 \longrightarrow \varprojlim A_i \xrightarrow{\alpha} \varprojlim B_i \xrightarrow{\beta} \varprojlim C_i \longrightarrow 1$$

exakt.

Beweis. Es ist nur noch die Exaktheit an der Stelle $\varprojlim B_i$ zu zeigen. Sei also $b = (\dots, b_i, \dots) \in \operatorname{im} \alpha$. Dann ist $b_i = \alpha_i(a_i)$ und folglich $\beta(b_i) = 1$, also $\beta(b) = 1$ und $b \in \ker \beta$. Ist umgekehrt $b \in \ker \beta$, so gilt $b_i = \alpha_i(a_i)$ für gewisse $a_i \in A_i$. Zu zeigen ist, daß $a = (\dots, a_i, \dots) \in A$ gilt. Dazu betrachten wir das kommutative Diagramm

$$\begin{array}{ccc} A_j & \xrightarrow{\pi_{ji}} & A_i \\ {\scriptstyle \alpha_j}\downarrow & & {\scriptstyle \alpha_i}\downarrow \\ B_j & \xrightarrow{\rho_{ji}} & B_i \end{array}$$

und rechnen $\alpha_i \circ \pi_{ji}(a_j) = (\alpha_i \circ \pi_{ji})(\alpha_j^{-1}(b_j)) = \rho_{ji} \circ \alpha_j(\alpha_j^{-1}(b_j)) = \rho_{ji}(b_j) = b_i$. Also ist $\pi_{ji}(a_j) = \alpha_i^{-1}(b_i) = a_i$, und das war zu zeigen. □

Der Satz bleibt richtig, wenn man ihn in der Kategorie der pro-endlichen Gruppen betrachtet: projektive Limites pro-endlicher Gruppen sind nämlich wieder pro-endlich (hätten wir die Charakterisierung pro-endlicher Gruppen als kompakte hausdorffsche und total unzusammenhängende Gruppen, wäre dies klar; andererseits läßt sich die Behauptung hier wohl auch mit einem Argument à la Cantorsches Diagonalverfahren beweisen).

Andererseits wird er falsch, wenn man ihn auf (unendliche) abelsche Gruppen anwendet: betrachten wir das exakte System, dessen n-te Zeile gegeben ist durch

$$0 \longrightarrow p^n\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0.$$

Dabei hat man rechts für $m \geq n$ die kanonischen Surjektionen $\mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$, in der Mitte die identischen Abbildungen, und links die durch $a \cdot$

$p^m\mathbb{Z} \longrightarrow (ap^{m-n}) \cdot p^n\mathbb{Z}$ definierten Einbettungen. Das projektive System dieser Gruppen (nicht Ringe! Die Projektionen in der linken Spalte sind keine Ringhomomorphismen) ist trivial, folglich ergibt sich im Limes die Sequenz

$$0 \longrightarrow 0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}_p \longrightarrow 0,$$

die rechts ersichtlich nicht mehr exakt ist.

Hier zeigt sich auch eine wesentliche Schwäche der Definition projektiver Systeme, bei welcher die Projektionen surjektiv sind: wir können in exakten Systemen wie oben im allgemeinen nicht ein projektives System so durch ein anderes ersetzen, daß die π_{ji} surjektiv werden *und* das ganze noch verträglich ist.

2.3 Eigenschaften pro-endlicher Gruppen

Offene Untergruppen pro-endlicher Gruppen haben immer endlichen Index:

Proposition 2.9. *Ist G kompakt und H offene Untergruppe, so ist $(G : H)$ endlich.*

Beweis. Es ist $\bigcup_{g\in G} gH$ eine offene Überdeckung von G, und G ist kompakt. □

Proposition 2.10. *Abgeschlossene Untergruppen H von pro-endlichen Gruppen G sind pro-endlich.*

Beweis. Sei $G = \varprojlim G_i$ und $U_i = \ker(G \longrightarrow G_i)$. Wir behaupten, daß die Gruppen HU_i/U_i ein projektives System bilden. Zuerst einmal ist die Ordnung von HU_i/U_i durch die Ordnung von $GU_i/U_i = G/U_i \simeq G_i$ nach oben beschränkt, und da G_i endlich ist, gilt dies auch für HU_i/U_i. Es genügt daher, $H \simeq \varprojlim HU_i/U_i$ (als topologischer Isomorphismus) zu zeigen. Die surjektiven Projektionen $H \longrightarrow HU_i/U_i$ liefern uns eine stetige Surjektion $\phi : H \longrightarrow \varprojlim HU_i/U_i$; diese ist injektiv: ist nämlich $h = (\dots, h_i, \dots) \in \ker\phi$, so liegt h_i im Kern von ϕ_i, d.h. es ist $\phi_i(h_i) = h + H \cap U_i$ trivial, somit $h \in H \cap U_i$ für alle i. Da die U_i eine Umgebungsbasis der 1 bilden und G hausdorffsch ist, gilt $\bigcap U_i = \{1\}$, folglich ist $h = 1$ und ϕ ein Isomorphismus. Da die Umgebungsbasen der 1 übereinstimmen, ist dieser Isomorphismus topologisch. □

Man beachte, daß wir im letzten Kapitel gesehen haben, daß dies für nicht abgeschlossene Untergruppen nicht gilt: ist G die pro-endliche Galoisgruppe von $\overline{F_p}/\mathbb{F}_p$ und H die vom Frobeniusautomorphismus σ erzeugte Untergruppe von G, so ist $H \simeq \mathbb{Z}$ keine pro-endliche Gruppe.

Analog gilt

Proposition 2.11. *Ist H eine abgeschlossene Untergruppen der pro-endlichen Gruppe G, so ist auch G/H pro-endlich; genauer ist $G/H \simeq \varprojlim G/HU_i$, wo $G = \varprojlim G_i$ und $U_i = \ker(G \longrightarrow G_i)$ ist.*

Wie im Falle endlicher Gruppen kann man auch bei pro-endlichen Gruppen einen Indexbegriff definieren. Dazu nennt man ein formales Produkt $\prod_p p^{n(p)}$ eine supernatürliche Zahl, wenn $0 \leq n(p) \leq \infty$ für alle Primzahlen p ist. Solche supernatürlichen Zahlen kann man zwar nicht addieren (für Indexrechnungen ist das auch gar nicht notwendig), aber die Multiplikation ist auf offensichtliche Weise definiert. Weiter kann man

$$\mathrm{ggT}\,(m,n) = \prod_p p^{\min\{m(p),n(p)\}} \text{ und } \mathrm{kgV}\,(\mathrm{m},\mathrm{n}) = \prod_{\mathrm{p}} \mathrm{p}^{\max\{\mathrm{m(p)},\mathrm{n(p)}\}}$$

setzen. Dasselbe geht natürlich für beliebig viele Elemente.

Ist G eine pro-endliche Gruppe, U_i das System der offenen Normalteiler von G, und H eine abgeschlossene Untergruppe von G, so ist $G = \varprojlim G/U_i$, und man setzt

$$(G : H) = \mathrm{kgV}\,(G/U_i : HU_i/U_i).$$

Die Indizes $(G/U_i : HU_i/U_i)$ sind endlich und damit wohldefiniert. Weiter setzt man $\#G = (G : 1)$. Beispielsweise ist $\#\mathbb{Z}_p = p^\infty$: die offenen Normalteiler von $\mathbb{Z}_p$ sind die $U_i = p^i\mathbb{Z}_p$, somit ist $G/U_i \simeq p^i\mathbb{Z}$, und das kgV aller $p^i = \#p^i\mathbb{Z}$ ist per definitionem p^∞.

Ist $\{U_j\}$ $(j \in J \subseteq I)$ irgendeine aus offenen Normalteilern bestehende Umgebungsbasis der 1, so ist J cofinal in I, und man überzeugt sich sofort davon, daß dann auch $(G : H) = \mathrm{kgV}\,(G/U_j : HU_j/U_j)$ ist.

Proposition 2.12. *Ist G eine pro-endliche Gruppe, und sind $K \subseteq H \subseteq G$ abgeschlossene Untergruppen, dann ist $(G : K) = (G : H)(H : K)$.*

Beweis. Sei $\{U_i\}$ wie in der Definition von $(G : H)$; dann ist

$$(G/U_i : KU_i/U_i) \;=\; (G/U_i : HU_i/U_i)(HU_i/U_i : KU_i/U_i). \tag{2.3}$$

Weiter bilden die $V_i = U_i \cap H$ eine aus offenen Normalteilern bestehende Umgebungsbasis der 1 in H; also ist

$$(H : K) \;=\; \mathrm{kgV}\,(H/V_i : KV_i/V_i).$$

Wegen $H/V_i = H/H \cap U_i \simeq HU_i/U_i$ und $KV_i/V_i \simeq K/K \cap V_i = K/K \cap U_i \simeq KU_i/U_i$ ist daher

$$(H : K) \;=\; \mathrm{kgV}\,(HU_i/U_i : KU_i/U_i).$$

Daraus folgt die Behauptung. □

Ganz entsprechend zeigt man

Proposition 2.13. *Ist G_i, π_{ji} ein projektives System, und sind alle π_{ji} surjektiv, so gilt $\#G = \mathrm{kgV}\ \#G_i$.*

Damit kann man die ganze Sylowtheorie endlicher Gruppen auf pro-endliche Gruppen übertragen: eine pro-endliche Gruppe G heißt pro-p-Gruppe, wenn sie projektiver Limes von endlichen p-Gruppen ist oder, was dasselbe ist, wenn $\#G$ eine p-Potenz ist. Beispielsweise ist $\mathbb{Z}_p$ eine pro-p-Gruppe. Eine abgeschlossene Untergruppe H einer pro-endlichen Gruppe G heißt p-Sylowgruppe, wenn H eine pro-p-Gruppe und $(G : H)$ nicht durch p teilbar ist. Damit gelten die ganz gewöhnlichen Sylowsätze:

Satz 2.14. *Sei G pro-endliche Gruppe. Dann existiert zu jeder Primzahl p eine p-Sylowgruppe G_p, und je zwei p-Sylowgruppen sind konjugiert. Jede pro-p-Untergruppe von G ist in einer p-Sylowgruppe enthalten. Schließlich ist $\#G = \prod_p \#G_p$.*

Ist L/K eine algebraische Körpererweiterung; dann kann man $(L : K)$ definieren als das kgV aller $(F : K)$, wobei F/K die endlichen Teilerweiterungen von L/K durchläuft. Die folgende Idee funktioniert dagegen nicht: wähle eine normale Erweiterung N/K $L \subseteq N$, und setze $(L : K) = (\mathrm{Gal}\,(N/K) : \mathrm{Gal}\,(N/L))$: das liegt daran, daß Quotienten supernatürlicher Zahlen nicht wohldefiniert sind. Aber für galoissche L/K gilt natürlich $\#\,\mathrm{Gal}\,(L/K) = (L : K)$.

Noch einige weitere Definitionen: ein Element g einer topologischen Gruppe G heißt topologische Erzeugende, wenn der Abschluß der von g algebraisch erzeugten Gruppe schon ganz G ist. Eine pro-endliche Gruppe G heißt pro-zyklisch, wenn sie projektiver Limes von zyklischen Gruppen ist; man kann zeigen, daß dies genau die pro-endlichen Gruppen sind, die von einem Element topologisch erzeugt werden. Die Gruppe $\mathbb{Z}_p$ ist pro-zyklisch.

Literatur

Das erste Kapitel des Buchs [2] von Koch gibt eine knappe Zusammenfassung von projektiven Limites und pro-endlichen Gruppen in der Sprache der Kategorientheorie. Eine ausführliche Diskussion pro-endlicher Gruppen findet man im Skript von Ribes [5], das auf einer Vorlesung von Neukirch basiert. Etwas gedrängter ist die Darstellung in Shatz [4], und in Wilson [6] findet man relativ viele Details. Wegen seiner Klarheit sei hier ausdrücklich die von Poitou herausgegebene Sammlung [3] erwähnt. Gruppentheoretische Probleme, die pro-endliche Gruppen betreffen (davon gibt es mehr als man glaubt), werden in [1] angesprochen.

1. J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal, *Analytic pro-p groups*, Cambridge Univ. Press 1991

2. H. Koch, *Galoissche Theorie der p-Erweiterungen*, Springer 1970

3. G. Poitou (ed.), *Cohomologie galoisienne des modules finies*, Sém. Inst. Math. Lille, 1967

4. Stephen S. Shatz, *Profinite groups, arithmetic, and geometry*, Annals of Math. Studies. 67, 1972

5. L. Ribes, *Introduction to profinite groups and Galois cohomology*, Kingston 1970

6. John S. Wilson, Profinite groups. London Mathematical Society Monographs, 1998

Kapitel 3

Kohomologiegruppen niedriger Dimension

3.1 Diskrete G-Moduln

Eine abelsche Gruppe heißt ein R-Modul, wenn R ein kommutativer Ring mit 1 ist und eine Abbildung $R \times A \longrightarrow A : (r, a) \longmapsto ra$ existiert mit folgenden Eigenschaften:

- $1a = a$ für alle $a \in A$;
- $(rs)a = r(sa)$ für alle $r, s \in R$, $a \in A$;
- $r(a + a') = ra + ra'$ für alle $r \in R$, $a, a' \in A$.

Insbesondere ist jede abelsche Gruppe ein $\mathbb{Z}$-Modul.

Ist G eine Gruppe, so heißt A ein G-Modul, wenn A ein $\mathbb{Z}[G]$-Modul ist, wo $\mathbb{Z}[G]$ den Gruppenring bezeichnet. Statt "A ist ein G-Modul" sagt man auch, G operiere auf A.

Sei L/K eine endliche Galoiserweiterung. Dann operiert $\mathrm{Gal}\,(L/K)$ z.B. auf L, auf $L^\times$, auf dem Ring ganzer Zahlen $\mathcal{O}_L$ in L, dessen Einheitengruppe E_L usw. usf. Geht man von L zu einer größeren Erweiterung N/K über, operiert $\mathrm{Gal}\,(N/K)$ auf diesen Gruppen, und bei jeder weiteren Erweiterung muß man die operierende Gruppe ebenfalls größer machen. Technisch einfacher ist es, stattdessen gleich $\mathrm{Gal}\,(\overline{K}/K)$ auf diesen Moduln operieren zu lassen, wo $\overline{K}$ der separable Abschluß von K ist. Diese oben betrachteten Moduln liegen in endlichen Erweiterungen von K, und das hat zur Folge, daß die Operation von $G = \mathrm{Gal}\,(\overline{K}/K)$ auf ihnen über einer offenen Untergruppe N faktorisiert: ist z.B. L/K endlich, so ist $U = \mathrm{Gal}\,(\overline{K}/L)$ eine offene Untergruppe von G, die auf L (oder $L^\times$, $\mathcal{O}_L$, E_L etc.) trivial operiert.

Tatsächlich funktioniert die Theorie etwas allgemeiner: man braucht nur, daß die Operation von G auf einem mit der diskreten Topologie versehenen Modul

A stetig ist. Wir wollen daher eine abelsche Gruppe A einen diskreten G-Modul nennen, wenn die durch die Operation definierte Abbildung $G \times A \longrightarrow A$ stetig ist, wobei A die diskrete und $G \times A$ die Produkttopologie trägt.

Man zeigt nun leicht

Lemma 3.1. *Sei G pro-endliche Gruppe und A abelsch; dann sind äquivalent:*

i) A ist diskreter G-Modul;

ii) der Stabilisator $G_a = \{\sigma \in G : a^\sigma = a\}$ von $a \in A$ ist offen in G;

iii) es ist $A = \bigcup_U A^U$, wobei $A^U = \{a \in a : a^\sigma = a \ \forall \sigma \in U\}$ ist.

Beweis. i) $\Longrightarrow$ ii): Sei $\phi : G \times A \longrightarrow A$ stetig; dann ist auch die Einschränkung $\overline{\phi} : G \times \{a\} \longrightarrow A$ stetig, folglich $G_a \times \{a\} = \overline{\phi}^{-1}(a)$ offen in $G \times \{a\}$ und damit G_a offen in G.

ii) $\Longrightarrow$ iii): Sei $a \in A$; da G_a offen ist, enthält es einen offenen Normalteiler U. Folglich ist $a = A^{G_a} \subseteq A^U$.

iii) $\Longrightarrow$ i): Sei $(\sigma, a) \in G \times \{a\}$ und $a^\sigma = b$; nach Voraussetzung ist $b \in A^U$ für einen offenen Normalteiler U. Dann ist $U\sigma \times \{a\}$ eine offene Umgebung von (σ, a) und $\phi(U\sigma \times \{a\}) = b$: also ist ϕ stetig. □

Faktorisiert die Operation von G auf einer abelschen Gruppe über einem offenen Normalteiler, so ist die Operation trivialerweise stetig. Weiter sieht man, daß Untermoduln und Quotientenmoduln diskreter Moduln wieder diskret sind. Dabei ist ein Untermodul B von A eine Untergruppe von A, welche gegenüber der Operation von G abgeschlossen ist; wegen ii) ist sicher auch B diskret. Ist B ein Untermodul, so operiert G auf der abelschen Gruppe $M = A/B$ durch $\sigma(aB) = \sigma(a)B$; wegen $\bigcup (A/B)^U = \bigcup (A^U/B) = A/B$ sind auch Quotienten diskreter Moduln wieder diskret.

Ein Homomorphismus zwischen G-Moduln heißt G-Homomorphismus, wenn er mit der Operation von G verträglich ist, wenn also $\phi(a^\sigma) = \phi(a)^\sigma$ gilt. Die Kategorie der diskreten G-Moduln wird mit $\mathrm{Mod}\,(G)$ bezeichnet; ihre Morphismen sind G-Homomorphismen abelscher Gruppen.

Da wir es weiter unten mit stetigen Abbildungen pro-endlicher Gruppen in diskrete Moduln zu tun haben werden, geben wir hier noch eine Charakterisierung der Stetigkeit:

Proposition 3.2. *Sei G pro-endliche Gruppe und A ein diskreter topologischer Raum. Eine Abbildung $f : G \longrightarrow A$ ist genau dann stetig, wenn es eine offene normale Untergruppe N von G gibt, sodaß f auf den Nebenklassen G/N konstant ist.*

Beweis. Sei f stetig. Dann ist $\{f^{-1}(a) : a \in A\}$ eine offene Überdeckung von G; da G kompakt ist, gibt es eine endliche Teilmenge B von A derart, daß G schon von $\{f^{-1}(a) : a \in B\}$ überdeckt wird. Für jedes $g \in f^{-1}(a)$ ist $g^{-1}f^{-1}(a)$

eine offene Umgebung der 1 in G und enthält folglich einen offenen Normalteiler V_g. Damit ist $gV_g \subseteq f^{-1}(a)$, und weil $f^{-1}(a)$ abgeschlossen ist, genügen endlich viele Mengen gV_g zur Überdeckung. Der Durchschnitt der dabei auftretenden offenen Normalteiler V_g sei N. Wegen $gV_g \subseteq f^{-1}(a)$ ist erst recht $gN \subseteq f^{-1}(a)$, also $f(gN) = a$.

Sei umgekehrt N eine offene normale Untergruppe von G und f auf den Nebenklassen G/N konstant. Dann ist $f^{-1}(a)$ eine Vereinigung gewisser (offenen) Mengen gN und damit offen. Also ist f stetig. □

Da offene Normalteiler pro-endlicher Gruppen immer endlichen Index besitzen, haben stetige Abbildungen wie oben also immer nur endlich viele Funktionswerte. Das legt auch folgende Konstruktion eines nicht diskreten Moduls nahe: wir setzen $L = \mathbb{Q}(\sqrt{\mathbb{N}})$ und $G = \mathrm{Gal}\,(L/\mathbb{Q})$; dann operiert die pro-endliche Gruppe G auf dem direkten Produkt $A = \prod_p \mathbb{Q}(\sqrt{p})$, wo das Produkt über alle Primzahlen geht. Wäre die Operation stetig, so müßte die Restriktion $G \times \{a\} \longrightarrow A$ der Operation eine stetige Abbildung sein, insbesondere dürfte ein Element $a \in A$ nur endliche viele Bilder unter der Operation von G haben. Das Element $a = (\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$ hat aber deren unendlich viele.

3.2 Das Schlangenlemma

Ein in Anwendungen oft auftretendes Problem ist folgendes: gegeben ist eine exakte Sequenz diskreter G-Moduln

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

und man interessiert sich für die Fixmoduln; man zeigt leicht, daß die Sequenz

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \tag{3.1}$$

immer exakt ist. Rechtsexaktheit gilt allerdings nicht immer: sei z.B. $K = \mathbb{Q}(\sqrt{3}\,)$, $G = \mathrm{Gal}\,(K/\mathbb{Q})$ und $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{3}$. Jedes Element $\alpha \in K^\times$ definiert ein Hauptideal (α), und man erhält die exakte Sequenz von G-Moduln

$$0 \longrightarrow E_K \longrightarrow K^\times \longrightarrow H_K \longrightarrow 0,$$

wo H_K die Gruppe der Hauptideale $\neq (0)$ bezeichnet. Die Fixmoduln von E_K und $K^\times$ sind offensichtlich $E_\mathbb{Q} = \{\pm 1\}$ und $\mathbb{Q}^\times$, während H_K^G strikt größer ist als $H_\mathbb{Q}$: beispielsweise sind die Hauptideale $(\sqrt{3}\,)$ und $(1+\sqrt{3}\,)$ beide invariant unter G; bei $(\sqrt{3}\,)$ ist das offensichtlich, bei $(1+\sqrt{3}\,)$ folgt dies aus $1-\sqrt{3} = -(1+\sqrt{3}\,)(1-\sqrt{3}\,) - (1+\sqrt{3}\,)$. Solche Ideale nennt man in der algebraischen Zahlentheorie übrigens verzweigt.

Kann man den Kokern der Abbildung $B^G \longrightarrow C^G$ angeben? Die Antwort lautet: fast. Die Idee ist, ein kommutatives Diagramm zu konstruieren, sodaß die Sequenz (3.1) der Anfang dessen ist, was uns das Schlangenlemma liefert.

Satz 3.3. *(Das Schlangenlemma) Sei ein kommutatives Diagramm*

$$\begin{array}{ccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array} \tag{3.2}$$

abelscher Gruppen (von G-Moduln) mit exakten Reihen gegeben. Dann existiert ein Homomorphismus (G-Homomorphismus) $\delta : \ker h \longrightarrow \operatorname{coker} f$ derart, daß die Sequenz

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker f & \longrightarrow & \ker\alpha & \longrightarrow & \ker\beta & \longrightarrow & \ker\gamma \\ & & & & & & & & \delta\downarrow \\ 0 & \longleftarrow & \operatorname{coker} g' & \longleftarrow & \operatorname{coker}\gamma & \longleftarrow & \operatorname{coker}\beta & \longleftarrow & \operatorname{coker}\alpha \end{array}$$

abelscher Gruppen (von G-Moduln) exakt wird.

Der Beweis ist, vermutlich bis auf die Exaktheit an Anfangs- und Endtermen, bekannt. Konstruieren wir also die Injektion $\ker f \longrightarrow \ker\alpha$. Sei dazu $a \in \ker f$; dann ist $\beta(f(a)) = 0$ wegen $f(a) = 0$. Die Kommutativität des Diagramms gibt $f'(\alpha(a)) = 0$, und da f' injektiv ist, folgt $\alpha(a) = 0$, d.h. $a \in \ker\alpha$. Die Konstruktion des Epimorphismus $\operatorname{coker}\gamma \longrightarrow \operatorname{coker} g'$ sowie die Exaktheit and den Stellen $\ker f$ und $\operatorname{coker} g'$ sind ebenso leicht, der Rest ist ohnehin bekannt.

Diese Version des Schlangenlemmas ist oft einfacher anzuwenden als die gewöhnliche. Hier ist ein Beispiel:

Korollar 3.4. *Seien $\alpha : A \longrightarrow B$ und $\beta : B \longrightarrow C$ Homomorphismen; dann gibt es eine exakte Sequenz*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker\alpha & \longrightarrow & \ker(\beta\circ\alpha) & \longrightarrow & \ker\beta \\ & & & & & & \downarrow \\ 0 & \longleftarrow & \operatorname{coker}\beta & \longleftarrow & \operatorname{coker}(\beta\circ\alpha) & \longleftarrow & \operatorname{coker}\alpha \end{array}$$

Beweis. Wende das Schlangenlemma auf folgendes Diagramm an:

$$\begin{array}{ccccccccc} & & A & \xrightarrow{\alpha} & B & \longrightarrow & \operatorname{coker}\alpha & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\beta\circ\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow & & \\ 0 & \longrightarrow & C & \xrightarrow{\mathrm{id}} & C & \longrightarrow & 0 & & \end{array}$$

□

3.3 Die erste Kohomologiegruppe

Zurück zum eigentlichen Thema. Unser Ziel ist, aus einer exakten Sequenz

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \tag{3.3}$$

diskreter G-Moduln ein kommutatives exaktes Diagramm

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & A^G & & B^G & & C^G & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C^1(G,A) & \longrightarrow & C^1(G,B) & \longrightarrow & C^1(G,C) & &
\end{array} \tag{3.4}$$

von (nicht notwendig diskreten) G-Moduln zu konstruieren; wir müssen dazu aus einem diskreten G-Modul A einen G-Modul $C^1(G,A)$ basteln, sowie einen G-Homomorphismus $A \longrightarrow C^1(G,A)$ konstruieren derart, daß der Kern genau aus A^G besteht. Das Schlangenlemma (angewandt in der Kategorie der G-Moduln) würde dann C^G in den Kokern von $A \longrightarrow C^1(G,A)$ abbilden; um an Hinweise zu kommen, wie wir $C^1(G,A)$ zu konstruieren haben, sollten wir uns also den Cokern von $\beta_* : B^G \longrightarrow C^G$ genauer ansehen. Sei dazu ein $c \in C^G$ gegeben; wegen der Surjektivität von β ist $c = \beta(b)$ für ein $b \in B$. Um die Tatsache $c \in C^G$ auszunutzen, lassen wir $\sigma \in G$ darauf los und finden $\beta(b^\sigma) = \beta(b)^\sigma = c^\sigma = c = \beta(b)$. Also ist $\beta(b - b^\sigma) = 0$, somit wegen der Exaktheit von (3.3) $b - b^\sigma \in A$ (hier haben wir A mit $\alpha(A)$ identifiziert).

Was zeigt uns das? Wir haben jedem $c \in C^G$ eine Abbildung $f_c : G \longrightarrow A$ zugeordnet, nämlich diejenige, welche $\sigma \in G$ auf $b - \sigma(b) \in A$ abbildet. Diese Abbildung $\psi : c \longmapsto f_c$ ist stetig: weil ψ ein Homomorphismus ist, genügt es, die Stetigkeit an der Stelle 0 zu zeigen. Das Urbild der 0 besteht aber aus allen σ, welche b fest lassen, d.h. es ist $f_c^{-1}(0) = G_b$ der Stabilisator von b, und der ist offen, weil A diskreter G-Modul ist. Was ist $f_c(\sigma\tau)$? Das kann man ausrechnen: $f_c(\sigma\tau) = b - \sigma\tau(b) = b - \sigma(b) + \sigma(b) - \sigma\tau(b) = \sigma(f_c(\tau)) + f_c(\sigma)$. Das einzige Unglück ist, daß $\delta(c)$ nicht wohldefiniert ist: wählt man nämlich ein anderes $b' \in B$ mit $\beta(b') = c$, so ist $b - b' =: a$ für ein $a \in A$, mit $\delta'(c) = b' - \sigma(b')$ folglich $\delta'(c) = \delta(c) + (a - \sigma(a))$. Daher ist $\delta(c)$ nur bis auf Abbildungen $G \longrightarrow A$ vom Typ $\sigma \longmapsto a - \sigma(a)$ definiert.

Die Idee ist daher,

$$C^1(G,A) \;=\; \{f : G \longrightarrow A \text{ stetig} : f(\sigma\tau) = \sigma f(\tau) + f(\sigma)\}$$

zu setzen und zu schauen, ob $C^1(G,A)$ unsere Erwartungen erfüllt. Zuerst einmal ist $C^1(G,A)$, wie jede Menge von Abbildungen in eine additive Gruppe, ebenfalls eine solche: wir erklären durch $(f+g)(\sigma) := f(\sigma)+g(\sigma)$ eine Addition, die Nullabbildung $0(\sigma)=0$ liefert das neutrale Element, und $(-f)(\sigma) := -f(\sigma)$ ist das zu f inverse Element. Falls G trivial auf A operiert, ist $C^1(G,A) = \mathrm{Hom}_c(G,A)$ gleich der Gruppe der (stetigen) Homomorphismen von G nach A. Die Elemente von $C^1(G,A)$ nennt man daher auch verschränkte Homomorphismen.

Weiter haben wir bereits gesehen, wie wir einen Homomorphismus $\psi : A \longrightarrow C^1(G,A)$ bekommen können: wir definieren $\psi(a)$ als diejenige stetige Abbildung $f_a : G \longrightarrow A$, welche σ auf $a-\sigma(a)$ abbildet. Diese Abbildung ist in der Tat ein verschränkter Homomorphismus (nachrechnen). Damit ist ψ ein Gruppenhomomorphismus, und sein Kern besteht aus allen $a \in A$, für welche $[\sigma \longmapsto a-\sigma(a)]$ die Nullabbildung ist, d.h. es ist $\ker\psi = A^G$.

Damit bleibt noch, $C^1(G,A)$ zu einem G-Modul zu machen. Dazu beachten wir, daß nicht nur A, sondern auch G selbst ein G-Modul ist, auf dem ein $\tau \in G$ durch Konjugation operiert: $c_\tau : \sigma \longrightarrow \tau\sigma\tau^{-1}$. Wegen $c_{\rho\tau}(\sigma) = \rho\tau\sigma\tau^{-1}\rho^{-1} = c_\rho(c_\tau(\sigma))$ ist dies in der Tat eine Operation (bei Operation von rechts hat man das Inverse auf die linke Seite zu schreiben). Wie soll nun $\tau \in G$ auf einer Abbildung $f : G \longrightarrow A$ operieren? Wir behaupten, daß $f^\tau := \tau \circ f \circ \tau^{-1}$ eine sinnvolle Definition ist. Zuerst einmal ist mit f auch f^τ stetig: f^τ ist nämlich Komposition der stetigen Abbildungen

$$G \xrightarrow{\tau^{-1}} G \xrightarrow{f} A \xrightarrow{\tau} A.$$

Weiter definiert dies wirklich eine G-Modulstruktur wegen

$$f^{\rho\tau}(\sigma) \;=\; \rho\tau(f(\tau^{-1}\rho^{-1}\sigma\rho\tau)) \;=\; \rho(f^\tau)(\rho^{-1}\sigma\rho) \;=\; (\rho(\tau f))(\sigma).$$

Als nächstes gilt es zu zeigen, daß f^τ die Kozykelrelation erfüllt: es ist aber

$$\begin{aligned} f^\tau(\rho\sigma) &= \tau f(\tau^{-1}\rho\sigma\tau) = \tau f(\tau^{-1}\rho\tau\tau^{-1}\sigma\tau) \\ &= \tau f(\tau^{-1}\rho\tau) + \tau\tau^{-1}\rho\tau f(\tau^{-1}\sigma\tau) = f^\tau(\rho) + \rho f^\tau(\sigma). \end{aligned}$$

Schließlich wird damit der Homomorphismus $\psi : A \longrightarrow C^1(G,A)$, welcher a auf $f_a : \sigma \longmapsto a - a^\sigma$ abbildet, zu einem G-Homomorphismus: es ist nämlich $\psi(a^\tau)(\sigma) = f_{\tau(a)}(\sigma) = \tau(a) - \sigma\tau(a)$ und $\psi(a)^\tau(\sigma) = f_a^\tau(\sigma) = \tau f_a(\tau^{-1}\sigma\tau) = \tau(a) - \tau\tau^{-1}\sigma\tau(a) = \tau(a) - \sigma\tau(a)$.

Wir behaupten dagegen nicht, daß der eben konstruierte G-Modul $C^1(G,A)$ diskret ist; das ist kein Beinbruch: die lange exakte Kohomologiesequenz macht auch für nicht diskrete G-Moduln Sinn. Warum dann die ganze Mühe mit der Stetigkeit? Die Antwort ist einfach: Kohomologiegruppen für nichtstetige G-Moduln lassen sich zwar einfach definieren, aber praktisch kaum berechnen. Wir werden das weiter unten noch genauer sehen.

Bemerkung. Man beachte, daß wir G von links auf der additiv geschriebenen Gruppe A operieren lassen. Würden wir A multiplikativ schreiben, so müßten wir $f(\sigma\tau) = f(\tau)^\sigma f(\sigma)$ fordern (wobei G immer noch von links operiert, trotz der nun exponentiellen Schreibweise). Lassen wir allerdings G von rechts auf der multiplikativen Gruppe A operieren, so wird daraus $f(\sigma\tau) = f(\sigma)^\tau f(\tau)$. Es ist also allergrößte Vorsicht angebracht, will man unsere Formeln auf Rechtsmoduln übertragen!

Die Zuordnung $A \longrightarrow C^1(G,A)$ ist funktoriell in folgendem Sinne: ist $\alpha : A \longrightarrow B$ ein G-Homomorphismus diskreter G-Moduln, so induziert α einen Homomorphismus $\alpha_* : C^1(G,A) \longrightarrow C^1(G,B) : f \longmapsto \alpha_*(f) = \alpha \circ f$. Damit gilt dann

Lemma 3.5. *Ist* $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ *eine exakte Sequenz diskreter* G*-Moduln, so ist*

$$0 \longrightarrow C^1(G,A) \longrightarrow C^1(G,B) \longrightarrow C^1(G,C)$$

eine exakte Sequenz von G*-Moduln.*

Beweis. Ist $\alpha \circ f \in C^1(G,B)$ die Nullabbildung, so ist wegen der Injektivität von α bereits f die Nullabbildung, also α_* injektiv.

Ist $f \in C^1(G,A)$, so ist $\beta \circ \alpha \circ f$ die Nullabbildung, weil $\beta \circ \alpha(a) = 0$ für alle $a \in A$ ist. Sei umgekehrt $g \in \ker \beta_*$, also $\beta \circ g(\sigma) = 0$ für alle $\sigma \in G$. Zu jedem $\sigma \in G$ gibt es daher ein $a_\sigma \in A$ mit $g(\sigma) = \alpha(a_\sigma)$. Wir definieren $f : G \longrightarrow A$ durch $f(\sigma) = a_\sigma$. Was ist $f(\sigma\tau)$? Wir wissen $g(\sigma\tau) = g(\sigma) + \sigma g(\tau)$, somit $\alpha(a_{\sigma\tau}) = \alpha(a_\sigma) + \sigma\alpha(a_\tau) = \alpha(a_\sigma + \sigma a_\tau)$ und damit $f(\sigma\tau) = a_{\sigma\tau} = a_\sigma + \sigma a_\tau$. Also ist $f \in C^1(G,a)$. □

Damit ist die Konstruktion des Diagramms (3.4) komplett. Das Bild des G-Homomorphismus $A \longrightarrow C^1(G,A)$ nennt man $B^1(G,A)$; seine Elemente heißen *zerfallende verschränkte Homomorphismen* oder 1-Koränder von G mit Werten in A. Der Kokern der Abbildung $A \longrightarrow C^1(A)$ ist damit gleich der Faktorgruppe $\mathrm{H}^1(G,A) := C^1(G,A)/B^1(G,A)$, die man die *erste Kohomologiegruppe* von G mit Werten in A nennt. Wendet man das Schlangenlemma auf das Diagramm (3.4) an, so erhält man

Proposition 3.6. *Zu jeder exakten Sequenz diskreter* G*-Moduln*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

existiert eine exakte Sequenz abelscher Gruppen

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow \mathrm{H}^1(G,A) \longrightarrow \mathrm{H}^1(G,B) \longrightarrow \mathrm{H}^1(G,C).$$

Die Abbildungen in der zweiten Sequenz kommen alle aus dem Schlangenlemma; insbesondere ist $\delta : C^G \longrightarrow \mathrm{H}^1(G,A)$ der Verbindungshomomorphismus. Damit ist die Sequenz $0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow 0$ sicher dann

exakt, wenn $\mathrm{H}^1(G,A)=0$ trivial ist. Allerdings ist dies keine notwendige Bedingung: notwendig und hinreichend für die Exaktheit ist vielmehr, daß der Homomorphismus $\mathrm{H}^1(G,A)\longrightarrow \mathrm{H}^1(G,B)$ injektiv ist.

Daß einen die G-Modulstruktur der Kohomologiegruppen nicht vom Hocker reissen wird kann man schon an $\mathrm{H}^0(G,A)=A^G$ sehen: das sind triviale G-Moduln. Dasselbe gilt, wie wir später sehen werden, für alle $\mathrm{H}^q(G,A)$ mit $q\geq 0$.

Wir wollen noch einige elementare, aber hilfreiche Bemerkungen über die erste Kohomologiegruppe machen. Ist A ein trivialer G-Modul (d.h. operiert G trivial auf A), so ist $C^1(A)=\mathrm{Hom}_c(G,A)$ sowie $B^1(A)=0$, und folglich $\mathrm{H}^1(G,A)\simeq \mathrm{Hom}_c(G,A)\simeq \mathrm{Hom}_c(G/G',A)$ (Letzteres, da A abelsch, jeder Homomorphismus $G\longrightarrow A$ daher G' auf die 0 abbildet). Ist insbesondere $A=\mathbb{Q}/\mathbb{Z}$, so ist $\mathrm{H}^1(G,\mathbb{Q}/\mathbb{Z})\simeq \mathrm{Hom}_c(G,\mathbb{Q}/\mathbb{Z})=X(G)$ die Charaktergruppe von G.

Proposition 3.7. *Ist $f:A\longrightarrow B$ ein G-Homomorphismus von G-Moduln, so induziert f einen Homomorphismus $f_*:\mathrm{H}^1(G,A)\longrightarrow \mathrm{H}^1(G,B)$.*

Beweis. Das kann man einmal direkt nachrechnen: sei $x\in C^1(G,A)$, also $x(\sigma\tau)=\sigma x(\tau)+x(\sigma)$ für alle $\sigma,\tau\in G$. Wir behaupten, daß dann $f\circ x\in C^1(G,B)$ ist. In der Tat gilt nämlich $(f\circ x)(\sigma\tau)=f(\sigma x(\tau)+x(\sigma))=\sigma(f\circ x)(\tau)+(f\circ x)(\sigma)$, Letzteres, da f ein G-Homomorphismus ist. Ebenso rechnet man nach, daß $f\circ x\in B^1(G,B)$ ist, wenn $x\in B^1(G,A)$ gilt: in der Tat ist $(f\circ x)(\sigma)=f(x(\sigma))=f(a-\sigma(a))=f(a)-\sigma f(a)$. Damit folgt nun, daß f einen Homomorphismus f_* der Faktorgruppen $C^1(G,A)/B^1(G,A)\longrightarrow C^1(G,B)/B^1(G,B)$ induziert, und das war behauptet.

Andererseits folgt dies auch per Schlangenlemma: dazu bildet man die zu $f:A\longrightarrow B$ gehörigen exakten Sequenzen $0\longrightarrow \ker f\longrightarrow A\longrightarrow \mathrm{im}\, f\longrightarrow 0$ und $0\longrightarrow \mathrm{im}\, f\longrightarrow B\longrightarrow \mathrm{coker}\, f\longrightarrow 0$, bildet die entsprechenden Kohomologiesequenzen und setzt dann die daraus resultierenden Abbildungen $\mathrm{H}^1(G,A)\longrightarrow \mathrm{H}^1(G,\mathrm{im}\, f)$ und $\mathrm{H}^1(G,\mathrm{im}\, f)\longrightarrow \mathrm{H}^1(G,B)$ einfach zusammen. □

Die erste Kohomologiegruppe für endliche G

Bevor wir loslegen, weisen wir darauf hin, daß die Werte eines $x\in C^1(G,A)$ an der Stelle 1 durch die Kozykelbedingung festgelegt ist: es gilt nämlich $x(1)=x(1\cdot 1)=x(1)+1x(1)$, also $x(1)=0$; wird A multiplikativ geschrieben, ist entsprechend $x(1)=1$.

Proposition 3.8. *Sei G endliche Gruppe der Ordnung n; dann ist $\mathrm{H}^1(G,A)$ eine Torsionsgruppe: sie wird von n annulliert.*

Beweis. Sei $x\in C^1(G,A)$ gegeben; wir müssen zeigen, daß $nx\in B^1(G,A)$ gilt. Nun ist $x(\tau)=x(\sigma^{-1}\sigma\tau)=x(\sigma^{-1})+\sigma^{-1}x(\sigma\tau)$; addiert man diese Gleichungen

über alle $\sigma \in G$ auf und setzt $a = \sum_{\sigma\in G} x(\sigma^{-1})$, so findet man

$$nx(\tau) = a + \sum_{\sigma\in G} \sigma^{-1}x(\sigma\tau) = a + \tau\Big(\sum_{\sigma\in G}(\sigma\tau)^{-1}x(\sigma\tau)\Big).$$

Mit σ durchläuft natürlich auch $\sigma\tau$ ganz G; weiter ist $0 = x(1) = x(\sigma^{-1}\sigma) = \sigma^{-1}x(\sigma) + x(\sigma^{-1})$, also $\sigma^{-1}x(\sigma) = -x(\sigma^{-1})$ und $\sum_{\sigma\in G}\sigma^{-1}x(\sigma) = -a$. Also folgt $nx(\tau) = a - \tau a$ für alle $\tau \in G$, und somit $nx \in B^1(G, A)$. □

Eine abelsche Gruppe M heißt dividierbar, wenn es für jedes $m \in M$ und jedes $n \in \mathbb{N}$ ein $m' \in M$ gibt mit $m = nm'$. Man nennt M eindeutig dividierbar, falls dieses m' eindeutig bestimmt ist.

Die Gruppe $(\mathbb{Q}, +)$ ist eindeutig dividierbar, $\mathbb{Q}/\mathbb{Z}$ zwar dividierbar, aber nicht eindeutig: es ist nämlich $0 + \mathbb{Z} = 2 \cdot (0 + \mathbb{Z}) = 2 \cdot (\frac{1}{2} + \mathbb{Z})$. Ebenso ist $\overline{\mathbb{Q}}^\times$, die multiplikative Gruppe des algebraischen Abschlusses von $\mathbb{Q}$, dividierbar (weil man n-te Wurzeln ziehen kann), aber nicht eindeutig (wegen der n-ten Einheitswurzeln).

Korollar 3.9. *Ist G endlich und A eindeutig dividierbar (also die Gleichung $ny = a$ für alle $a \in A$ und $n \in \mathbb{N}$ eindeutig lösbar), so ist* $\mathrm{H}^1(G, A) = 0$.

Beweis. Die kurze exakte Sequenz

$$0 \longrightarrow A \xrightarrow{n} A \longrightarrow 0 \longrightarrow 0$$

liefert

$$0 \longrightarrow \mathrm{H}^1(G, A) \xrightarrow{n} \mathrm{H}^1(G, A) \longrightarrow \mathrm{H}^1(G, 0) = 0,$$

d.h. Multiplikation mit n induziert einen Automorphismus von $\mathrm{H}^1(G, A)$; da $\mathrm{H}^1(G, A)$ Torsionsgruppe ist, muß $\mathrm{H}^1(G, A) = 0$ sein. □

Eine äußerst wichtige Beobachtung ist die folgende, die für zyklische Gruppen G sehr oft die Berechnung der doch etwas unhandlichen Gruppe $\mathrm{H}^1(G, A)$ erlaubt; dazu setzen wir $\nu = 1 + \sigma + \ldots + \sigma^{n-1}$ (wo n die Ordnung von G bezeichnet), und definieren ${}_\nu A = \{a \in A : \nu a = 1\}$ als den Teilmodul von A, der von der 'Norm' ν (eigentlich ist ν ja die Spur; da in den meisten Anwendungen aber A eine multiplikative Gruppe ist, ist dieser Sprachmissbrauch recht geläufig) annulliert wird. Offenbar ist $A^{1-\sigma} = \{a^{1-\sigma} : a \in A\}$ ein Teilmodul von ${}_\nu A$, und wir können den Faktormodul $\widehat{\mathrm{H}}^{-1}(G, A) = {}_\nu A/A^{1-\sigma}$ definieren (in der Tat kann man diesen Modul als eine -1^{te} Kohomologiegruppe im Tateschen Sinne interpretieren). Jetzt gilt

Proposition 3.10. *Ist G zyklisch und endlich, so gilt* $\mathrm{H}^1(G, A) \simeq {}_\nu A/I_G A$.

Beweis. Sei σ eine Erzeugende von G (der zu konstruierende Isomorphismus wird von der Wahl von σ abhängen, ist also nicht kanonisch). Wir behaupten, daß $\phi : C^1(G, A) \longrightarrow A : x \longmapsto x(\sigma)$ in ${}_\nu A$ landet. In der Tat ist nämlich

$x(\sigma^k) = x(\sigma) + \sigma x(\sigma^{k-1}) = \ldots = \sum_{j=0}^{k-1} \sigma^j x(\sigma)$, also insbesondere $\nu x(\sigma) = x(\sigma^n) = x(1) = 0$. Damit induziert ϕ einen Homomorphismus $\overline{\phi} : C^1(G,A) \simeq {}_\nu A/I_G A$. Zu zeigen ist, daß der Kern gerade $B^1(G,A)$ und daß $\overline{\phi}$ surjektiv ist.

Ist $x \in B^1(G,A)$, also $x(\sigma) = a - \sigma(a)$, so ist offenbar $\phi(x) = a - \sigma(a) \in I_G A$. Gilt umgekehrt $\phi(x) \in I_G A$, also $x(\sigma) = a - \sigma(a)$ für die Erzeugende σ von G, so folgt induktiv $x(\sigma^2) = \sigma x(\sigma) + x(\sigma) = \sigma(a - \sigma(a)) + a - \sigma(a) = a - \sigma^2(a)$ etc., also $x(\tau) = a - \tau(a)$ für alle $\tau \in G$ und damit $x \in B^1(G,A)$.

Zur Surjektivität: sei $a \in {}_\nu A$ gegeben. Gesucht ist ein x mit $x(\sigma) = a$. Dies verwenden wir als Definition; damit wird nämlich $x(\sigma^2) = x(\sigma)^{1+\sigma} = a^{1+\sigma}, \ldots,$ und schließlich $x(\sigma^n) = a^{1+\sigma+\ldots+\sigma^{n-1}} = a^\nu = 1$, was wegen $1 = x(1) = x(\sigma^n)$ auch gut so ist. Jetzt muß man noch nachrechnen, daß die dadurch definierte Abbildung $G \longrightarrow A$ ein 1-Kozykel ist: das ist aber nicht schwer. Ist z.B. $i + j < n$, so folgt $x(\sigma^i\sigma^j) = a^{1+\sigma+\ldots+\sigma^{i+j}}$, andererseits gibt $x(\sigma^i)\sigma^i x(\sigma^j)$ genau dasselbe. Die Fälle $i + j = n$ und $i + j > n$ behandelt man genauso. □

Es ist klar, daß jeder Versuch, Proposition 3.10 auf proendliche Gruppen zu übertragen, scheitern muß, weil $\sum_{\sigma \in G}$ für nichtendliche G keinen großen Sinn macht. Dagegen ist die Behauptung, $\mathrm{H}^1(G,A)$ sei Torsionsgruppe, durchaus sinnvoll, und tatsächlich gilt:

Proposition 3.11. *Sei G eine pro-endliche Gruppe und A ein diskreter G-Modul; dann ist $\mathrm{H}^1(G,A)$ eine Torsionsgruppe.*

Beweis. Der Beweis ist derselbe wie im endlichen Fall, zuzüglich eines kleinen Tricks: wir nehmen wie oben ein $x \in C^1(G,A)$ her und beachten, daß x stetig ist. Folglich existiert ein offener Normalteiler N von G derart, daß $x(\sigma) = x(\sigma N)$ für alle $\sigma \in G$ gilt. Die Addition über alle $\sigma \in G$ wird hier über alle $\sigma \in G/N$ geführt, und mit $n = (G : N)$ folgt wie im endlichen Fall, daß $nx \in B^1(G,A)$ liegt. Man beachte aber, daß n von x abhängt; es ist also nicht gesagt, daß es eine natürliche Zahl gibt, welche $\mathrm{H}^1(G,A)$ annulliert! □

Ein Beispiel

Sei $K = \mathbb{Q}(\sqrt{m}\,)$ ein reellquadratischer Zahlkörper mit Ring ganzer Zahlen $\mathcal{O}_K$; die Einheitengruppe $E_K = \mathcal{O}_K^\times$ hat nach Dirichlet (bzw. Pell und Fermat) die Struktur $E_K = \langle -1 \rangle \times \langle \varepsilon \rangle$, wobei ε eine Fundamentaleinheit heißt. Da Einheiten die ganzen Elemente der Norm 1 sind, gilt $N\varepsilon = +1$ oder $N\varepsilon = -1$, und beide Fälle kommen vor: für $m = 3$ ist $\varepsilon = 2 + \sqrt{3}$, für $m = 5$ dagegen $\varepsilon = \frac{1}{2}(1 + \sqrt{5}\,)$.

Was können wir nun über die Kohomologiegruppe $\mathrm{H}^1(G, E_K)$ sagen, wo $G = \mathrm{Gal}\,(K/\mathbb{Q}) = \{1, \sigma\}$ die Galoisgruppe von $K/\mathbb{Q}$ ist? Ihre Vertreter sind verschränkte Homomorphismen $f : G \longrightarrow E_K$. Wir haben bereits gesehen, daß $f(1) = 1$ gelten muß, daher ist f durch seinen Wert an der Stelle σ festgelegt. Setzen wir also an $f(\sigma) = (-1)^a \varepsilon^b$ mit $0 \le a \le 1$ und $b \in \mathbb{Z}$. Welche dieser Abbildungen liefern verschränkte Homomorphismen? Offenbar

muß $1 = f(1) = f(\sigma^2) = f(\sigma) \cdot \sigma f(\sigma) = (-1)^a \varepsilon^b \cdot (-1)^a \varepsilon^{b\sigma} = \varepsilon^{(1+\sigma)b}$ gelten. In der Tat ist dies auch hinreichend dafür, daß f verschränkter Homomorphismus ist, weil die andern Relationen $f(1 \cdot \sigma) = f(\sigma) = f(\sigma \cdot 1)$ automatisch erfüllt sind.

Ist daher $N\varepsilon = \varepsilon^{1+\sigma} = +1$, so definiert $f(\sigma) = (-1)^a \varepsilon^b$ immer einen verschränkten Homomorphismus, im Falle $N\varepsilon = -1$ dagegen genau dann, wenn b gerade ist.

Die Gruppe $C^1(G, E_K)$ ist also recht groß (sie enthält $\mathbb{Z}$); andererseits ist $B^1(G, A)$ fast ebenso groß: diese Gruppe besteht aus Abbildungen, die die $1 \in G$ auf die $1 \in E_K$ und $\sigma \longmapsto \eta^{1-\sigma}$ für ein $\eta \in E_K$ abbilden. Da man $\eta^{1-\sigma} = \varepsilon^{b(1-\sigma)}$ schreiben kann, und da weiter $\varepsilon^{1-\sigma} = \varepsilon^2/\varepsilon^{1+\sigma}$ gilt, haben wir $f(\sigma) = \varepsilon^{2b}$ mit $b \in \mathbb{Z}$ im Falle $N\varepsilon = +1$, und $f(\sigma) = (-\varepsilon^2)^b$ mit $b \in \mathbb{Z}$ im Falle $N\varepsilon = -1$. Es ist jetzt eine leichte Übung, daraus $\mathrm{H}^1(G, E_K)$ zu berechnen:

Proposition 3.12. *Sei K reellquadratischer Zahlkörper mit Einheitengruppe E_K, $G = \mathrm{Gal}\,(K/\mathbb{Q})$ seine Galoisgruppe und ε seine Fundamentaleinheit. Dann ist*

$$\mathrm{H}^1(G, E_K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{falls } N\varepsilon = -1, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{falls } N\varepsilon = +1. \end{cases}$$

Tatsächlich hätten wir das viel billiger haben können: da G zyklisch ist, gilt $\mathrm{H}^1(G, E_K) = {}_N E_K / E_K^{1-\sigma}$, und wir erhalten dasselbe Ergebnis ohne große Rechnung. Wir bemerken ebenfalls, daß wir das Ergebnis unserer Rechnung in der Form

$$\#\mathrm{H}^1(G, E_K) = 2(E_{\mathbb{Q}} : NE_K) \tag{3.5}$$

zusammenfassen können. Übrigens ist die Gruppe $E_{\mathbb{Q}}/NE_K = E_{\mathbb{Q}}^G/NE_K \simeq \widehat{\mathrm{H}}^0(G, E_K)$ die nullte Kohomologiegruppe im Tateschen Sinne (sh. unten). Als Übungsaufgabe zeige man $\mathrm{H}^1(G, E_K) \simeq \mathbb{Z}/2\mathbb{Z}$, falls K ein imaginärquadratischer Zahlkörper ist. Dessen Einheiten bestehen aus den in K liegenden Einheitswurzeln W_K, und es ist $\#W_K = 4, 6$ oder 2, je nachdem $\mathrm{disc}\, K = -4, -3$ oder < -4 ist.

Das Berechnen der ersten Kohomologie der Einheitengruppe galoisscher (ja sogar nur zyklischer) Erweiterungen von Zahlkörpern ist ein *zentrales Problem* der algebraischen Zahlentheorie, genauer der Klassenkörpertheorie. Die Kraft solcher Resultate wird in folgendem Beispiel überhaupt nicht deutlich: sei K wie oben; dann erhalten wir aus

$$1 \longrightarrow E_K \longrightarrow K^\times \longrightarrow H_K \longrightarrow 1$$

mit Hilbert 90 die Kohomologiesequenz

$$\mathbb{Q}^\times \longrightarrow H_K^G \longrightarrow \mathrm{H}^1(G, E_K) \longrightarrow 1,$$

also den Isomorphismus $H_K^G/H_{\mathbb{Q}} \simeq \mathrm{H}^1(G, E_K)$. Mit anderen Worten: $\mathrm{H}^1(G, E_K)$ mißt die Abweichung der G-invarianten Hauptideale in K von denjenigen, welche von rationalen Zahlen erzeugt werden. Im Falle $K = \mathbb{Q}(\sqrt{3})$ hatten wir bereits gesehen, daß $(\sqrt{3})$ und $(1+\sqrt{3})$ Ideale sind, deren Klassen in $H_K^G/H_{\mathbb{Q}}$ nichttrivial sind; das obige Ergebnis besagt, daß alle solchen Ideale Produkte von Potenzen dieser beiden Ideale sind.

Kummertheorie

Ein wichtiges (und gleichzeitig das älteste) Ergebnis der Galoiskohomologie ist Hilberts Satz 90: dieses taucht für Erweiterungen $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ bereits als Hilfssatz bei Kummer auf; Hilbert hat es dann in seinem Zahlbericht in den Rang eines Satzes erhoben (den 90. seines Berichts). Die folgende Formulierung wird in sämtlichen Quellen Emmy Noether zugeschrieben; Falko Lorenz hat sich kürzlich die entsprechende Arbeit einmal angesehen und festgestellt (siehe [2]), daß Noether dabei auf eine Arbeit von Andreas Speiser verweist, in der die entsprechenden Resultate über verschränkte Produkte (sogar in etwas allgemeinerer Form als bei Noether) enthalten sind.

Proposition 3.13. *Hilberts Satz 90: Sei L/K eine normale Körpererweiterung mit $G = \mathrm{Gal}\,(L/K)$. Dann ist $\mathrm{H}^1(G, L^\times) = 1$.*

Beweis. Sei zuerst L/K endlich. Da $L^\times$ eine multiplikative Gruppe ist, gehen wir für den G-Modul $L^\times$ zu einer multiplikativen Schreibweise über. Sei $x \in C^1(G, L^\times)$, und betrachte $b = \sum_{\sigma\in G} x(\sigma)\sigma(c)$ für $c \in L^\times$. Da die Autmorphismen von L/K unabhängig sind, existiert ein $c \in L^\times$, für welches $b \neq 0$ ist. Damit ist dann (beachte, daß wegen der multiplikativen Schreibweise von $L^\times$ nun $x(\tau\sigma) = \tau x(\sigma) \cdot x(\tau)$ gilt)

$$\tau b = \sum_{\sigma\in G} \tau x(\sigma)\tau\sigma(c) = \sum_{\sigma\in G} x(\tau\sigma)x(\tau)^{-1}\tau\sigma(c) = x(\tau)^{-1}b,$$

also $x(\tau) = b^{1-\tau}$ und damit $x \in B^1(G, L^\times)$.

Die Modifikation für unendliche Erweiterungen sollte klar sein: da $L^\times$ ein diskreter G-Modul ist, gibt es zu $x \in C^1(G, L^\times)$ einen offenen Normalteiler N, sodaß x auf den Nebenklassen von G/N konstant ist. Statt über alle $\sigma \in G$ bildet man das Produkt über alle $\sigma \in G/N$. □

Hilberts ursprüngliche (auf Kummer zurückgehende) Version lautet

Korollar 3.14. *Sei L/K eine endliche zyklische Erweiterung, und σ eine Erzeugende von $G = \mathrm{Gal}\,(L/K)$. Dann ist genau dann $N_{L/K}\alpha = 1$, wenn es ein $\beta \in L^\times$ mit $\alpha = b^{1-\sigma}$ gibt.*

Beweis. Da G endlich und zyklisch ist, gilt $1 = \mathrm{H}^1(G, L^\times) \simeq \mathrm{H}^{-1}(G, L^\times) \simeq {}_NL^\times/(L^\times)^{1-\sigma}$ nach Proposition 3.10; daraus folgt die Behauptung sofort. □

Kummertheorie für endliche Erweiterungen

Wir wollen zum Vergleich einmal die Kummertheorie einmal für endliche Erweiterungen, dann mit Hilfe pro-endlicher Gruppen herleiten.

Eine Körpererweiterung L/K heißt kummersch, wenn L/K abelsch mit einer Galoisgruppe G vom Exponenten n ist, und wenn K die Gruppe μ_n der n-ten Einheitswurzeln enthält. Damit ist gemeint, daß die Gruppe μ_n aller n-ten Einheitswurzeln Ordnung n hat; insbesondere folgt, daß die Charakteristik von K entweder 0 oder kein Teiler von n ist: ist nämlich ζ_p eine p-te Einheitswurzel in einem Körper der Charakteristik p, so folgt aus $(x-\zeta_p)^p = x^p - 1 = (x-1)^p$, daß $\zeta_p = 1$ ist! Insbesondere operiert G trivial auf μ_n, folglich ist $X(G) = \mathrm{Hom}(G, \mu_n) = \mathrm{H}^1(G, \mu_n)$. Erheben von $\alpha \in L^\times$ in die n^{te} Potenz liefert eine exakte Sequenz

$$1 \longrightarrow \mu_n \longrightarrow L^\times \xrightarrow{n} (L^\times)^n \longrightarrow 1,$$

welche die folgende Kohomologiesequenz induziert:

$$K^\times \xrightarrow{n} L^{\times n} \cap K \xrightarrow{\delta} \mathrm{H}^1(G, \mu_n) \longrightarrow \mathrm{H}^1(G, L^\times).$$

Aufbrechen der Sequenz liefert wegen $\mathrm{H}^1(G, L^\times) = 1$

$$1 \longrightarrow K^{\times n} \longrightarrow L^{\times n} \cap K \xrightarrow{\delta} \mathrm{H}^1(G, \mu_n) \longrightarrow 1,$$

also den Isomorphismus $(L^{\times n} \cap K)/K^{\times n} \simeq \mathrm{H}^1(G, \mu_n) = X(G)$. Dabei rechnet man ohne weiteres nach, daß die Nebenklasse $aK^{\times n} \in (L^{\times n} \cap K)/K^{\times n}$ auf den Charakter $\chi_a(\sigma) = (\alpha)^{1-\sigma}$ abgebildet wird, wobei $a = \alpha^n$ ist und die Wahl der n-ten Wurzel beliebig ist, da G trivial auf den n-ten Einheitswurzeln operiert. In der Tat, haben wir ein solches Element in $(L^{\times n} \cap K)/K^{\times n}$ gegeben, so müssen wir dessen Bild unter dem Verbindungshomomorphismus δ des Schlangenlemmas finden; das dazugehörige Diagramm ist

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_n & \longrightarrow & K^\times & \longrightarrow & L^{\times n} \cap K^\times & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_n & \longrightarrow & L^\times & \longrightarrow & L^{\times n} & \longrightarrow & 1 \\
 & & \downarrow 0 & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Hom}(G, \mu_n) & \longrightarrow & C^1(G, L^\times) & \longrightarrow & C^1(G, L^{\times n}) & &
\end{array}$$

[Man überzeuge sich davon, daß die Abbildung $\mu_n \longrightarrow C^1(G, \mu_n) = \mathrm{Hom}(G, \mu_n)$ wirklich die Nullabbildung ist!] Wir starten mit $a \in L^{\times n} \cap K^\times$ und schreiben $a = \alpha^n$ mit $\alpha \in L^\times$ (jetzt sind wir in der mittleren Reihe in $L^{\times n}$). Zurückgehen auf $L^\times$ bedeutet, $\alpha \in L^\times$ herzunehmen, und dieses α wird jetzt nach $\mathrm{Hom}(G, L^\times)$ abgebildet, indem man ihm den Homomorphismus $\chi_\alpha : \sigma \longmapsto$

$\alpha^{1-\sigma}$ zuordnet. Dies ist in der Tat ein Homomorphismus wegen $\chi_\alpha(\sigma)\chi_\alpha(\tau) = \chi_\alpha(\sigma)\chi_\alpha(\tau)^\sigma = \alpha^{1-\sigma}\alpha^{\sigma-\sigma\tau} = \chi_\alpha(\sigma\tau)$. Insbesondere ist $\chi_\alpha(\sigma)^n = \chi_\alpha(\sigma^n) = 1$, folglich sogar $\chi_\alpha(\sigma) \in \mu_n$ und damit $\chi_\alpha \in \mathrm{Hom}(G, \mu_n)$ wie erwartet.

Der Rest der Kummertheorie wird wie üblich abgewickelt.

Proposition 3.15. *Ist L/K eine Kummererweiterung mit $G = \mathrm{Gal}\,(L/K)$, so ist $X(G) \simeq (L^{\times n} \cap K)/K^{\times n}$. Teilerweiterungen von L/K entsprechen dabei Untergruppen von $(L^{\times n} \cap K)/K^{\times n}$.*

Kummertheorie für beliebige Kummererweiterungen

Hier sei K *irgendein* Körper, welcher eine primitive n-te Einheitswurzel ζ_n enthält. Sei weiter $\overline{K}$ der separable Abschluß von K und $G = \mathrm{Gal}\,(\overline{K}/K)$. Die zugrundegelegte exakte Sequenz ist hier

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{\ n\ } \overline{K}^\times \longrightarrow 1.$$

Hier haben wir benutzt, daß Potenzieren mit n auf $\overline{K}$ ein Epimorphismus mit Kern μ_n ist! Die exakte Kohomologiesequenz plus Hilberts Satz 90 liefert

$$K^\times \xrightarrow{\ n\ } K^\times \longrightarrow \mathrm{H}^1(G, \mu_n) \longrightarrow 1,$$

also den Isomorphismus $\mathrm{Hom}_c(G, \mu_n) \simeq K^\times/K^{\times n}$.

Ein anderer Zugang ist folgender: wir starten mit einem stetigen Charakter von $G = \mathrm{Gal}\,(L/K)$ mit Werten in $K^\times$, also einem Homomorphismus $\chi : G \longrightarrow K^\times$. Da G trivial auf $K^\times$ operiert, ist $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau) = \chi(\sigma)\chi(\tau)^\sigma$ ein verschränkter Homomorphismus in $C^1(G, L^\times)$. Da die erste Kohomologie von $L^\times$ trivial ist, muß $\chi \in B^1(G, L^\times)$ sein, d.h. es gibt ein $\alpha \in L^\times$ mit $\chi(\sigma) = \alpha^{1-\sigma}$. Wegen $1 = \chi(\sigma)^n = (\alpha^n)^{1-\sigma}$ muß $\alpha^n \in K^\times$ sein.

Mit $A = \{\alpha \in L^\times : \alpha^n \in K^\times\}$ hat also jeder stetige Charakter $\chi \in X(G)$ die Form $\chi = \chi_\alpha$ für ein geeignetes $\alpha \in A$. Umgekehrt ist χ_α für jedes $\alpha \in A$ ein stetiger Charakter: die Homomorphieeigenschaft haben wir bereits einmal vorgerechnet, und die Stetigkeit ist klar, weil χ auf $\mathrm{Gal}\,(L/K(\alpha))$ trivial ist. Setzt man $(a, \sigma) := \alpha^{1-\sigma}$, so definiert dieses Symbol eine Paarung $A \times G \longrightarrow \mu_n$, die bekannte Kummer-Paarung.

3.4 Die Tateschen Gruppen $\widehat{\mathrm{H}}^0$ und $\widehat{\mathrm{H}}^{-1}$

Ist G eine endliche Gruppe und A ein G-Modul, und bezeichnet $N = \sum_{\sigma\in G} \sigma$ die Norm (bzw. die Spur, falls A additiv geschrieben wird). Mit ${}_N A$ bezeichnen wir den Untermodul von A, der von N annulliert wird. Ist

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1 \tag{3.6}$$

eine exakte Sequenz von G-Moduln und setzt man $\mathrm{H}_0(G,A) := A/I_G A$, so rechnet man nach, daß auch die Sequenz

$$\mathrm{H}_0(G,A) \longrightarrow \mathrm{H}_0(G,B) \longrightarrow \mathrm{H}_0(G,C) \longrightarrow 1$$

exakt ist. Damit können wir das Schlangenlemma auf das Diagramm

$$\begin{array}{ccccccccc} & & \mathrm{H}_0(G,A) & \longrightarrow & \mathrm{H}_0(G,B) & \longrightarrow & \mathrm{H}_0(G,C) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \\ 1 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \longrightarrow & \mathrm{im}\,\delta \end{array}$$

anwenden und erhalten so die exakte Sequenz

$$\begin{aligned} {}_N A/I_G A &\longrightarrow {}_N B/I_G B \longrightarrow {}_N C/I_G C \longrightarrow \\ A^G/NA &\longrightarrow B^G/NB \longrightarrow C^G/NC \longrightarrow \mathrm{im}\,\delta \longrightarrow 1. \end{aligned}$$

Setzen wir also $\widehat{\mathrm{H}}^{-1}(G,A) = {}_N A/I_G A$ und $\widehat{\mathrm{H}}^0(G,A) = A^G/NA$, und verkleben wir die eben erhaltene Sequenz mit

$$1 \longrightarrow \mathrm{im}\,\delta \longrightarrow \mathrm{H}^1(G,A) \longrightarrow \mathrm{H}^1(G,B) \longrightarrow \dots,$$

so haben wir gezeigt:

Proposition 3.16. *Ist G eine endliche Gruppe, so existiert zu jeder exakten Sequenz (3.6) von G-Moduln eine lange exakte Sequenz*

$$\begin{aligned} \widehat{\mathrm{H}}^{-1}(G,A) &\longrightarrow \widehat{\mathrm{H}}^{-1}(G,B) \longrightarrow \widehat{\mathrm{H}}^{-1}(G,C) \longrightarrow \\ \widehat{\mathrm{H}}^{0}(G,A) &\longrightarrow \widehat{\mathrm{H}}^{0}(G,B) \longrightarrow \widehat{\mathrm{H}}^{0}(G,C) \longrightarrow \\ \mathrm{H}^{1}(G,A) &\longrightarrow \mathrm{H}^{1}(G,B) \longrightarrow \mathrm{H}^{1}(G,C). \end{aligned}$$

Selbstverständlich lassen sich die Aussagen von Prop. 3.7 und 3.8 problemlos auf die beiden Tateschen Kohomologiegruppen der Dimensionen 0 und -1 ausdehnen. Da wir uns damit später ganz allgemein befassen werden, sei dies dem Leser hier als Übungsaufgabe überlassen. Im nächsten Abschnitt zeigen wir die kleinen Kohomologiegruppen in Aktion.

3.5 Geschlechtertheorie quadratischer Zahlkörper

Bevor wir loslegen, stellen wir zwei kleine Ergebnisse bereit:

Proposition 3.17. *Ist L/K eine endliche normale Erweiterung von Zahlkörpern mit $G = \mathrm{Gal}\,(L/K)$, so ist $\widehat{\mathrm{H}}^{-1}(G, I_L) = 1$.*

Beweis. $\widehat{\mathrm{H}}^{-1}(G, I_L)$ ist die Faktorgruppe der Gruppe der Ideale mit Relativnorm (1) modulo der Gruppe von Idealen der Form $\mathfrak{a} = \mathfrak{b}_1^{1-\sigma_1} \cdots \mathfrak{b}_t^{1-\sigma_t}$. Wir schreiben $\mathfrak{a} \in {}_N I_L$ als Quotienten $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ ganzer Ideale $\mathfrak{b}, \mathfrak{c}$; ist $\mathfrak{P}$ ein Primideal, welches $\mathfrak{b}$ teilt, so muß ein zu $\mathfrak{P}$ konjugiertes Primideal $\mathfrak{c}$ teilen, d.h. es gibt ein $\sigma \in G$ mit $\mathfrak{P}^\sigma \mid \mathfrak{c}$. Also ist $\mathfrak{b} = \mathfrak{P}\mathfrak{b}'$, $\mathfrak{c} = \mathfrak{P}^\sigma \mathfrak{c}'$, und $\mathfrak{a} = \mathfrak{P}^{1-\sigma}\mathfrak{b}'/\mathfrak{c}'$. Indem wir so fortfahren, finden wir schließlich, daß $\mathfrak{a}$ die gewünschte Form besitzt: das Verfahren muß nämlich abbrechen, weil ein ganzes Ideal nur endlich viele Primideale als Teiler besitzt. □

Ist L/K eine normale Erweiterung mit $G = \mathrm{Gal}\,(L/K)$, so ist der Fixmodul von L, $L^\times$ oder E_L natürlich K, $K^\times$, bzw. E_K. Dagegen gilt für Ideale

Proposition 3.18. *Sei L/K eine normale Erweiterung mit $G = \mathrm{Gal}\,(L/K)$; dann ist $I_L^G/I_K \simeq \bigoplus \mathbb{Z}/e_\mathfrak{p}\mathbb{Z}$, wo $e_\mathfrak{p}$ den Verzweigungsindex eines Primideal $\mathfrak{p}$ in L/K bezeichnet.*

Beweis. Sei $\mathfrak{A} \in I_L^G$; ist $\mathfrak{P}$ ein Primideal, welches $\mathfrak{A}$ teilt, dann muß $\mathfrak{A}$ durch alle Konjugierten von $\mathfrak{P}$ teilbar sein. Ist $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{e_\mathfrak{p}}$ die Primidealzerlegung von $\mathfrak{p}$ in $\mathcal{O}_L$, so muß also $\mathfrak{A} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)\mathfrak{B}$ für ein ganzes Ideal $\mathfrak{B} \in I_L^G$ gelten. Induktion zeigt dann, daß wir $\mathfrak{A}$ als Produkt $\mathfrak{A} = \prod_\mathfrak{p} (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{a_\mathfrak{p}}$ schreiben können, und jetzt behaupten wir, daß $\mathrm{cl} : \mathfrak{A} I_K \longmapsto (\dots, a_\mathfrak{p} + e_\mathfrak{p}\mathbb{Z}, \dots)$ ein wohldefinierter Homomorphismus $\mathrm{cl} : I_L^G/I_K \longrightarrow \bigoplus \mathbb{Z}/e_\mathfrak{p}\mathbb{Z}$ ist. In der Tat, ist $\mathfrak{p} \in I_K$, so wird $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{e_\mathfrak{p}}$ auf 0 abgebildet.

Schließlich besteht $\ker \mathrm{cl}$ aus all denen Idealen $\mathfrak{A}$, für die $a_\mathfrak{p} = e_\mathfrak{p}$ für alle Primideale $\mathfrak{p} \in I_K$ gilt. Dies sind aber genau die Ideale aus I_K, d.h. cl ist injektiv. Da cl offensichtlich surjektiv ist, folgt die Behauptung. □

Nun zum eigentlichen Thema: sei K ein quadratischer Zahlkörper und $G = \mathrm{Gal}\,(K/\mathbb{Q})$ seine Galoisgruppe, weiter I_K die Gruppe der Ideale (also die Halbgruppe der Ideale in $\mathcal{O}_K$, die z.B. durch Einführung künstlicher Inversen zur Gruppe gemacht wird), H_K die Untergruppe der Hauptideale, und $\mathrm{Cl}(K) = I_K/H_K$ die Idealklassengruppe. Per definitionem ist die Sequenz

$$1 \longrightarrow H_K \longrightarrow I_K \longrightarrow \mathrm{Cl}(K) \longrightarrow 1$$

exakt, und bilden der Kohomologie liefert

$$I_K^G \longrightarrow \mathrm{Cl}(K)^G \longrightarrow \mathrm{H}^1(G, H_K) \longrightarrow \mathrm{H}^1(G, I_K)$$

Da $G = \langle\sigma\rangle$ zyklisch ist, gilt $\mathrm{H}^1(G, I_K) = {}_N I_K/I_K^{1-\sigma}$, wo $N = 1 + \sigma$ die Norm bedeutet. Jetzt gilt Hilberts Satz 90 für Ideale, und es folgt dann

$$1 \longrightarrow I_K^G/H_K^G \longrightarrow \mathrm{Cl}_K^G \longrightarrow \mathrm{H}^1(G, H_K) \longrightarrow 1,$$

und damit also

$$\#\mathrm{Cl}_K^G = (I_K^G : H_K^G)\#\mathrm{H}^1(G, H_K). \tag{3.7}$$

Den ersten Index formen wir um:

$$(I_K^G : H_K^G) = \frac{(I_K^G : H_\mathbb{Q})}{(H_K^G : H_\mathbb{Q})} = \frac{(I_K^G : I_\mathbb{Q})(I_\mathbb{Q} : H_\mathbb{Q})}{(H_K^G : H_\mathbb{Q})} = \frac{2^t}{(H_K^G : H_\mathbb{Q})}, \tag{3.8}$$

wobei wir $(I_K^G : I_\mathbb{Q})$ aus Proposition 3.18 bekommen und $(I_\mathbb{Q} : H_\mathbb{Q}) = 1$ aus der Tatsache, daß $\mathbb{Q}$ Klassenzahl 1 hat. Weiter lesen wir aus der exakten Sequenz

$$1 \longrightarrow E_\mathbb{Q} \longrightarrow \mathbb{Q}^\times \longrightarrow H_K^G \longrightarrow \mathrm{H}^1(G, E_K) \longrightarrow 1$$

ab, daß $(H_K^G : H_\mathbb{Q}) = \#\mathrm{H}^1(G, E_K) = \#\widehat{\mathrm{H}}^{-1}(G, E_K)$ ist, und diese Ordnung haben wir zu $\#\widehat{\mathrm{H}}^{-1}(G, E_K) = 2(E_\mathbb{Q} : NE_K)$ berechnet. Also ist

$$(H_K^G : H_\mathbb{Q}) = 2(E_\mathbb{Q} : NE_K). \tag{3.9}$$

Zusammenfassend haben wir damit

$$\#\mathrm{Cl}_K^G = \frac{2^{t-1}}{(E_\mathbb{Q} : NE_K)} \#\mathrm{H}^1(G, H_K).$$

Um den letzten Faktor zu verarzten, benutzen wir ersten die Tatsache, daß $\mathrm{H}^1(G, H_K) \simeq \widehat{\mathrm{H}}^{-1}(G, H_K)$ ist, weil G zyklisch ist, und zur Berechnung von $\#\widehat{\mathrm{H}}^{-1}(G, H_K)$ beuten wir die Sequenz

$$\widehat{\mathrm{H}}^{-1}(G, K^\times) \longrightarrow \widehat{\mathrm{H}}^{-1}(G, H_K) \longrightarrow \widehat{\mathrm{H}}^0(G, E_K) \longrightarrow \widehat{\mathrm{H}}^0(G, K^\times)$$

aus (wo die herkommt, ist nicht schwer zu sehen). Da G zyklisch ist, gilt $\widehat{\mathrm{H}}^{-1}(G, K^\times) \simeq \mathrm{H}^1(G, K^\times) = 1$ mit Hilbert 90, folglich $\#\widehat{\mathrm{H}}^{-1}(G, H_K)$ gleich dem Quotienten von $\#\widehat{\mathrm{H}}^0(G, E_K)$ modulo der Ordnung des Bilds der Abbildung $[\widehat{\mathrm{H}}^0(G, E_K) \longrightarrow \widehat{\mathrm{H}}^0(G, K^\times)]$. Wie sieht dieses aus?

Betrachten wir ganz allgemein Untergruppen A und D einer abelschen Gruppe B und fragen, wie das Bild von A unter der Projektion $B \longrightarrow B/D$ aussieht. Bekanntlich haben die Untergruppen von B/D die Form UD/D, wo U die Untergruppen von B durchläuft; insbesondere ist das Bild von A damit gleich AD/D.

Im Falle $\widehat{\mathrm{H}}^0(G, E_K) = E_K^G/NE_K = E_\mathbb{Q}/NE_K$ und $\widehat{\mathrm{H}}^0(G, K^\times) = \mathbb{Q}^\times/NK^\times$ ist dann

$$\mathrm{im}\,[\widehat{\mathrm{H}}^0(G, E_K) \longrightarrow \widehat{\mathrm{H}}^0(G, K^\times)] = E_\mathbb{Q} NK^\times/NK^\times \simeq E_\mathbb{Q}/E_\mathbb{Q} \cap NK^\times,$$

folglich $\#\widehat{\mathrm{H}}^{-1}(G, H_K) = (E_\mathbb{Q} : NE_K)/(E_\mathbb{Q} : E_\mathbb{Q} \cap NK^\times)$ und damit endlich

$$\#\mathrm{Cl}_K^G = \frac{2^{t-1}}{(E_\mathbb{Q} : NE_K)} \#\mathrm{H}^1(G, H_K) = \frac{2^{t-1}}{(E_\mathbb{Q} : E_\mathbb{Q} \cap NK^\times)}.$$

Wir haben bewiesen (der imaginärquadratische Fall ist wieder eine einfache Übungsaufgabe):

Satz 3.19. *Sei $K/\mathbb{Q}$ eine quadratische Erweiterung, und sei t die Anzahl der verzweigten Ideale, also der Primteiler der Diskriminante* disc K*. Dann gilt*

$$\#\mathrm{Cl}_K^G = \begin{cases} 2^{t-1}, & \text{falls } K \text{ imaginär,} \\ \frac{2^{t-1}}{(E_{\mathbb{Q}}:E_{\mathbb{Q}}\cap NK^\times)}, & \text{falls } K \text{ reell} \end{cases}$$

also $\#\mathrm{Cl}_K^G = 2^{t-1}$ falls disc K *negativ oder Summe zweier Quadrate ist, und $\#\mathrm{Cl}_K^G = 2^{t-2}$ sonst.*

In der Tat: ist -1 Norm einer Zahl aus K, also $-1 = x^2 - dy^2$, so ist $(-1/p) = +1$ für jeden ungeraden Primteiler p von d, also d Summe zweier Quadrate; ist umgekehrt $d = a^2 + b^2$, so ist -1 die Norm von $(a + \sqrt{d}\,)/b$.

Wir bemerken außerdem, daß der ganze Beweis auch für zyklische Erweiterungen von Primzahlgrad p durchgeht: das einzige Problem ist die Bestimmung von $\#\mathrm{H}^1(G, E_K)$.

Noch eine kleine Beobachtung:

Lemma 3.20. *Sei $G = \langle\sigma\rangle$ eine Gruppe der Ordnung 2 und A ein endlicher G-Modul, welcher von $1 + \sigma$ annulliert wird. Dann ist $\#A^G = (A : A^2)$.*

Beweis. Wir betrachten die exakte Sequenz

$$1 \longrightarrow A^G \longrightarrow A \longrightarrow A^{1-\sigma} \longrightarrow 1.$$

Da $1 + \sigma$ angewandt auf A alles annulliert, operiert σ wie -1, folglich ist $A^{1-\sigma} = A^2$. Jetzt folgt die Behauptung. □

Sei nun $p \equiv 1 \bmod 4$ prim. Dann gibt es genau ein verzweigtes Primideal in $K = \mathbb{Q}(\sqrt{p}\,)$, folglich ist $\mathrm{Cl}_K^G = 1$. Da die Norm $1+\sigma$ jedes Ideal zum Hauptideal macht, muß nach dem Lemma $(\mathrm{Cl}_K : \mathrm{Cl}_K^2) = 1$ sein, d.h. Quadrieren ist ein Automorphismus von Cl_K. Also hat Cl_K ungerade Ordnung h.

Ist jetzt q eine ungerade Primzahl mit $(p/q) = +1$, so ist q in K zerlegt: $q\mathcal{O}_K = \mathfrak{q}\mathfrak{q}'$ (in der Tat: sei $p \equiv x^2 \bmod q$; dann ist $\mathfrak{q} = (q, x + \sqrt{p}\,)$ ein Primideal, welches q teilt). Damit ist $\mathfrak{q}^h = \frac{1}{2}(r + s\sqrt{p}\,)$ Hauptideal, und Normenbildung liefert $q^h = \pm(r^2 - ps^2)/4$. Reduziert man diese Gleichung modulo p, so folgt $q^h \equiv \pm r^2 \bmod p$. Wegen $(-1/p) = +1$ und weil h ungerade ist, folgt daraus aber $(q/p) = +1$. Mit anderen Worten: ist $p \equiv 1 \bmod 4$ und $(p/q) = +1$, so folgt $(q/p) = +1$. Das ist ein Spezialfall des quadratischen Reziprozitätsgesetzes; die anderen Fälle können analog bewiesen werden (ein vollständiger Beweis, allerdings in der Sprache der Idealklassengruppe im engeren Sinne geschrieben, steht in meinem Skript über quadratische Zahlkörper). Für Primzahlen $p \equiv 3 \bmod 4$ benutzt man, daß $\mathbb{Q}(\sqrt{-p}\,)$ ungerade Klassenzahl hat.

Eine andere Möglichkeit ist diese: seien $p \equiv q \equiv 3 \bmod 4$ prim. Dann ist -1 keine Norm aus $K = \mathbb{Q}(\sqrt{pq}\,)$, weil $x^2 - pqy^2 = -z^2$ mit $(x, y, z) = 1$ sofort $(x/z)^2 \equiv -1 \bmod p$ impliziert, was wegen $p \equiv 3 \bmod 4$ nicht sein kann. Also ist $(E_{\mathbb{Q}} : E_{\mathbb{Q}} \cap NE_K) = 2$, somit die Klassenzahl h von K ungerade. Nun ist

aber mit $\mathfrak{p} = (p, \sqrt{pq}\,)$ verzweigt: $\mathfrak{p}^2 = (p^2, p\sqrt{pq}, pq) = p(p, \sqrt{pq}, q) = (p)$. Da $\mathfrak{p}^2$ ein Hauptideal und die Klassenzahl ungerade ist, muß schon $\mathfrak{p}$ Hauptideal sein. Also gibt es $X, y \in \mathbb{Z}$ mit $\pm 4p = X^2 - pqy^2$. Mit $X = px$ gibt das $\pm 4 = px^2 - qy^2$. Das Vorzeichen ist bestimmt durch $\pm 1 = (p/q)$, wie man durch Reduktion modulo q sofort feststellt. Reduktion modulo p liefert dagegen $(-q/p) = \pm 1$, und es folgt $(p/q) = -(q/p)$.

Dieser Beweis geht auf den zweiten Gaußschen Beweis zurück, der in der Sprache der binären quadratischen Formen geschrieben ist; die Formel für Cl_K^G entspricht dort die Formel für die Anzahl der Geschlechter quadratischer Formen.

Literatur

Als erste Einführung in die Kohomologie von Gruppen ist Weiss [4] zu empfehlen; deutlich sparsamer in Details sind dagegen die Bücher von Lang [1] und Serre [3].

Einen analytischen Zugang zur Geschlechtertheorie quadratischer Zahlkörper bietet Zagier [5]. Die vorhandenen Bücher über die klassische Theorie binärer quadratischer Formen sind durch die Bank schlecht.

1. S. Lang, *Topics in cohomology of groups*, Springer-Verlag, Berlin, 1996; frz. Original *Rapport sur la cohomologie des groupes*, Benjamin, Inc. 1967

2. F. Lorenz, *Ein Scholion zum Satz 90 von Hilbert*, Abh. Math. Sem. Univ. Hamburg **68** (1998), 347–362

3. Jean-Pierre Serre, *Galois cohomology*, Springer 1997; *Cohomologie Galoisienne*, Lecture Notes Math. 5, 1973

4. E. Weiss, *Cohomology of groups*, Academic Press, New York-London 1969

5. D. Zagier, *Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*, Springer-Verlag 1981

Kapitel 4
Die lange Kohomologiesequenz

In diesem Kapitel geht es darum, etwas mehr kohomologische Maschinerie bereitzustellen.

4.1 Die lange exakte Kohomologiesequenz

Die Entwicklungen in diesem Abschnitt sind rein formal; alle Aussagen gelten sowohl für beliebige G-Moduln, Abbildungen, Kozykeln etc. wie auch für diskrete G-Moduln und stetige Abbildungen, Kozykeln etc.

Eine Sequenz von G-Moduln

$$\ldots \longrightarrow V_{n-1} \xrightarrow[d_n]{} V_n \xrightarrow[d_{n+1}]{} V_{n+1} \longrightarrow \ldots$$

heißt ein Kokettenkomplex V^*, wenn $d_{n+1} \circ d_n = 0$ für alle $n \in \mathbb{Z}$ gilt; man schreibt hierfür auch kurz $dd = 0$. Wegen $\operatorname{im} d_n \subseteq \ker d_{n+1}$ können wir die Faktormoduln $\mathrm{H}^n(V^*) = \ker d_{n+1} / \operatorname{im} d_n$ definieren; diese werden die Kohomologiemoduln von V^* genannt. Die Menge $\{d_n\}$ der Modulhomomorphismen heißt das Differential des Komplexes V^*.

Komplexe sind uns bereits wohlbekannt: jede exakte Sequenz

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \tag{4.1}$$

können wir nämlich via

$$\ldots \longrightarrow 0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \longrightarrow \ldots$$

als Komplex auffassen (indem wir z.B. $V_0 = A$ setzen), der eben nur an drei Stellen nichttrivial ist. Bildet man die zu (4.1) gehörige Sequenz der Fixmoduln

$$\ldots \longrightarrow 0 \longrightarrow A^G \xrightarrow{\iota} B^G \xrightarrow{\pi} C^G \longrightarrow 0 \longrightarrow , \ldots$$

so ist auch dies ein Komplex, wenn auch vielleicht kein exakter. Tatsächlich messen die dazugehörigen Kohomologiegruppen die Abweichung des Komplexes von der Exaktheit: mit $V_0 = A^G$ wird nämlich $\mathrm{H}^0(V^*) = \ker \imath/0 = 0$, $\mathrm{H}^1(V^*) = \ker \pi / \operatorname{im} \imath = 0$, sowie $\mathrm{H}^2(V^*) = C^G / \operatorname{im} \pi = \operatorname{coker} \pi$. Die Kohomologiegruppen dieses Komplexes sind also höchstens an der Stelle C^G nichttrivial; und zwar ist $\mathrm{H}^2(V^*) = 0$ genau dann, wenn der Komplex exakt ist.

Jetzt wollen wir darangehen, die Kohomologiegruppen $\mathrm{H}^n(G, A)$ für alle $n \in \mathbb{N}$ zu konstruieren. Dazu setzen wir $\mathrm{K}^n(G, A) = \operatorname{Abb}_c(G^n, A)$ für $n \geq 1$, wo $\operatorname{Abb}_c(G^n, A)$ die additive Gruppe der stetigen Abbildungen $G^n \longrightarrow A$ ist, und $\mathrm{K}^0(G, A) = A$ (d.h. ein $x \in \operatorname{Abb}_c(G^0, A)$ wird mit dem Bild $x(\cdot) = a$ identifiziert). Für alle $n \geq 0$ konstruieren wir jetzt Homomorphismen $d_{n+1} : \mathrm{K}^n(G, A) \longrightarrow \mathrm{K}^{n+1}(G, A)$ via

$$\begin{aligned}(d_{n+1}x)(\sigma_1, \ldots, \sigma_{n+1}) \;&=\; \sigma_1 x(\sigma_2, \ldots, \sigma_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i x(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \sigma_{i+2}, \ldots, \sigma_{n+1}) \\ &\quad + (-1)^{n+1} x(\sigma_1, \ldots, \sigma_n).\end{aligned}$$

Insbesondere ist $d_1 x(\sigma) = \sigma x(\cdot) - x(\cdot) = \sigma(a) - a$: dies sind gerade zerfallende 1-Kozyklen (abgesehen von einem Vorzeichen, das natürlich keine Rolle spielt), deren Kern der Fixmodul A^G ist. Weiter ist $(d_2 x)(\sigma, \tau) = \sigma x(\tau) - x(\sigma\tau) + x(\sigma)$, d.h. $\ker d_2$ sind gerade die verschränkten Homomorphismen.

Alles hängt jetzt davon ab nachzuweisen, daß

$$0 \xrightarrow{d_0} \mathrm{K}^0(G, A) \xrightarrow{d_1} \mathrm{K}^1(G, A) \xrightarrow{d_2} \mathrm{K}^2(G, A) \xrightarrow{d_3} \ldots$$

ein Komplex ist, d.h. daß $d_{n+1} \circ d_n = 0$ ist. Haben wir das getan, so können wir die Kohomologiegruppen dieses Komplexes einfach durch $\mathrm{H}^n(G, A) := \ker d_{n+1} / \operatorname{im} d_n$ definieren. Damit ist dann

- $\mathrm{H}^0(G, A) = \ker d_1 / \operatorname{im} d_0 = A^G$, da $\operatorname{im} d_0 = 0$ ist;
- $\mathrm{H}^1(G, A) = \ker d_2 / \operatorname{im} d_1 = \frac{\{\text{verschränkte Homomorphismen}\}}{\{\text{zerfallende verschr. Homomorphismen}\}}$

in Übereinstimmung mit unseren früheren Definitionen. Der Interpretation von $\mathrm{H}^2(G, A)$ werden wir den nächsten Abschnitt widmen, sodaß wir uns jetzt um den Nachweis von $dd = 0$ kümmern können.

Es ist natürlich möglich, dies mit roher Gewalt direkt nachzurechnen; ein klein wenig Mühe kann man sich jedoch sparen, wenn man die Kohomologiegruppen durch homogene Koketten beschreibt. Wir setzen dazu

$$\mathrm{K}^n_{\mathrm{h}}(G, A) = \{x : G^{n+1} \longrightarrow A \mid x(\sigma\sigma_0, \ldots, \sigma\sigma_n) = \sigma x(\sigma_0, \ldots, \sigma_n)\}.$$

Offenbar ist $\mathrm{K}_{\mathrm{h}}^n(G,A)$ eine Untergruppe von $\mathrm{K}^{n+1}(G,A)$, die wir die Gruppe der *homogenen Koketten* nennen werden. Für diese definieren wir Korand-Operatoren $\partial_{n+1} : \mathrm{K}_{\mathrm{h}}^n(G,A) \longrightarrow \mathrm{K}_{\mathrm{h}}^{n+1}(G,A)$ durch

$$(\partial_{n+1}x)(\sigma_0,\dots,\sigma_{n+1}) = \sum_{i=0}^{n+1}(-1)^i x(\sigma_0,\dots,\widehat{\sigma_i},\dots,\sigma_{n+1}),$$

wobei die Tarnkappe über $\widehat{\sigma_i}$ bedeuten soll, daß diese (i^{te}) Koordinate ausgelassen wird. Damit ist z.B.

- $(\partial_1 x)(\sigma_0,\sigma_1) = x(\sigma_1) - x(\sigma_0)$,
- $(\partial_2 x)(\sigma_0,\sigma_1,\sigma_2) = x(\sigma_1,\sigma_2) - x(\sigma_0,\sigma_2) + x(\sigma_0,\sigma_1)$.

Der Nachweis von $\partial\partial = 0$ ist hier nicht so schwer:

$$(\partial_{n+1}\partial_n x)(\sigma_0,\dots,\sigma_{n+1}) = \sum_{i=0}^{n+1}(-1)^i \partial_n x(\sigma_0,\dots,\widehat{\sigma_i},\dots,\sigma_{n+1}).$$

Nun ist aber

$$\begin{aligned}\partial_n x(\sigma_0,\dots,\widehat{\sigma_i},\dots,\sigma_{n+1}) \;&=\; \sum_{j<i}(-1)^j x(\sigma_0,\dots,\widehat{\sigma_j},\dots,\widehat{\sigma_i},\dots,\sigma_{n+1}) \\ &\quad + \sum_{j>i}(-1)^{j-1} x(\sigma_0,\dots,\widehat{\sigma_i},\dots,\widehat{\sigma_j},\dots,\sigma_{n+1}),\end{aligned}$$

$$\begin{aligned}\text{also}\quad (\partial_{n+1}\partial_n x)(\sigma_0,\dots,\sigma_{n+1}) = \\ \sum_{i=0}^{n+1}(-1)^i \sum_{j<i}(-1)^j x(\sigma_0,\dots,\widehat{\sigma_j},\dots,\widehat{\sigma_i},\dots,\sigma_{n+1}) \\ + \sum_{i=0}^{n+1}(-1)^i \sum_{j>i}(-1)^{j-1} x(\sigma_0,\dots,\widehat{\sigma_i},\dots,\widehat{\sigma_j},\dots,\sigma_{n+1}).\end{aligned}$$

In dieser Summe kommt jedes $x(\sigma_0,\dots,\widehat{\sigma_i},\dots,\widehat{\sigma_j},\dots,\sigma_{n+1})$ genau zweimal vor, allerdings mit umgekehrtem Vorzeichen. Also ist wie behauptet $\partial\partial = 0$ und K_{h}^* ein Komplex.

Für den Nachweis, daß auch $dd = 0$ ist, genügt es, Isomorphismen $\phi_n : \mathrm{K}^n(G,A) \longrightarrow \mathrm{K}_{\mathrm{h}}^n(G,A)$ bzw. $\psi_n : \mathrm{K}_{\mathrm{h}}^n(G,A) \longrightarrow \mathrm{K}^n(G,A)$ anzugeben, sodaß das folgende Diagramm kommutativ ist:

$$\begin{array}{ccc} \mathrm{K}^n(G,A) & \xrightarrow{d_{n+1}} & \mathrm{K}^{n+1}(G,A) \\ \psi_n \downarrow \uparrow \phi_n & & \psi_{n+1} \downarrow \uparrow \phi_{n+1} \\ \mathrm{K}_{\mathrm{h}}^n(G,A) & \xrightarrow{\partial_{n+1}} & \mathrm{K}_{\mathrm{h}}^{n+1}(G,A) \end{array}$$

In der Tat wird dann wegen $d_n = \phi_n \partial_n \psi_{n-1}$ nämlich

$$d_{n+1} d_n = \phi_{n+1} \partial_{n+1} \psi_n \phi_n \partial_n \psi_{n-1} = \phi_{n+1} \partial_{n+1} \partial_n \psi_{n-1} = 0.$$

Zur Konstruktion der Isomorphismen setzen wir

$$\begin{aligned} (\phi_n x)(\sigma_1, \dots, \sigma_n) &= x(1, \sigma_1, \sigma_1\sigma_2, \dots, \sigma_1 \cdots \sigma_n) \quad \text{und} \\ (\psi_n y)(\tau_0, \dots, \tau_n) &= \tau_0 y(\tau_0^{-1}\tau_1, \tau_1^{-1}\tau_2, \dots, \tau_{n-1}^{-1}\tau_n) \end{aligned}$$

für $x \in K_h^n(G, A)$ und $y \in K^n(G, A)$. Zuerst rechnen wir nach, daß $\psi_n y$ wirklich homogen ist:

$$(\psi_n y)(\tau\tau_0, \dots, \tau\tau_n) = \tau\tau_0 y(\tau_0^{-1}\tau_1, \dots, \tau_{n-1}^{-1}\tau_n) = \tau(\psi_n y)(\tau_0, \dots, \tau_n).$$

Zweitens behaupten wir, daß $\phi_n \circ \psi_n$ und $\psi_n \circ \phi_n$ die identischen Abbildungen sind. Mit $f = \phi_n x$ folgt ersteres aus

$$\begin{aligned} (\psi_n \phi_n x)(\tau_0, \dots, \tau_n) &= (\psi_n f)(\tau_0, \dots, \tau_n) &&= \tau_0 f(\tau_0^{-1}\tau_1, \dots, \tau_{n-1}^{-1}\tau_n) \\ &= \tau_0 x(1, \tau_0^{-1}\tau_1, \dots, \tau_0^{-1}\tau_n) &&= x(\tau_0, \dots, \tau_n), \end{aligned}$$

wobei wir verwendet haben, daß x homogen ist. Mit $g = \psi_n y$ folgt entsprechend

$$\begin{aligned} (\phi_n \psi_n y)(\sigma_1, \dots, \sigma_n) &= (\phi_n g)(\sigma_1, \dots, \sigma_n) \\ &= g(1, \sigma_1, \sigma_1\sigma_2, \dots, \sigma_1 \cdots \sigma_n) \\ &= 1 \cdot y(\sigma_1, \dots, \sigma_n). \end{aligned}$$

Als nächstes zeigen wir, daß die ϕ_n und ψ_n mit den Korandoperatoren vertauschbar sind:

$$\begin{aligned} (\psi_n d_n x)(\sigma_0, \dots, \sigma_n) &= \sigma_0 (d_n x)(\sigma_0^{-1}\sigma_1, \dots, \sigma_0^{-1}\sigma_n) \\ &= \sigma_1 x(\sigma_1^{-1}\sigma_2, \dots, \sigma_{n-1}^{-1}\sigma_n) \\ &\quad + \sum_{i=1}^{n-1} (-1)^i \sigma_0 x(\sigma_0^{-1}\sigma_1, \dots, \sigma_{i-1}^{-1}\sigma_{i+1}, \dots, \sigma_{n-1}^{-1}\sigma_n) \\ &\quad + (-1)^n \sigma_0 x(\sigma_0^{-1}\sigma_1, \dots, \sigma_{n-2}^{-1}\sigma_{n-1}), \quad \text{sowie} \\ (\partial_n \psi_{n-1} x)(\sigma_0, \dots, \sigma_n) &= \sum_{i=0}^{n} (-1)^i (\psi_{n-1} x)(\sigma_0, \dots, \widehat{\sigma_i}, \dots, \sigma_n) \\ &= \sigma_1 x(\sigma_1^{-1}\sigma_2, \dots, \sigma_{n-1}^{-1}\sigma_n) \\ &\quad + \sum_{i=1}^{n-1} (-1)^i \sigma_0 x(\sigma_0^{-1}\sigma_1, \dots, \sigma_{i-1}^{-1}\sigma_{i+1}, \dots, \sigma_{n-1}^{-1}\sigma_n) \\ &\quad + (-1)^n \sigma_0 x(\sigma_0^{-1}\sigma_1, \dots, \sigma_{n-2}^{-1}\sigma_{n-1}), \end{aligned}$$

und da beide Ausdrücke übereinstimmen, folgt unsere Behauptung. Mit $\psi_n d_n = \partial_n \psi_{n-1}$ ist natürlich erst recht $\psi_n d_n \phi_{n-1} = \partial_n \psi_{n-1} \phi_{n-1} = \partial_n$, folglich auch

$d_n\phi_{n-1} = \phi_n\psi_n d_n\phi_{n-1} = \phi_n\partial_n$, d.h. die zweite Vertauschungsrelation ist eine Folge aus der ersten.

Insbesondere ist damit $dd = 0$. Damit folgt nicht nur, daß K^* ein Komplex ist, sondern darüberhinaus $C^n(G,A) = \ker d_{n+1} \simeq \ker \partial_{n+1} = C^n_{\mathrm{h}}(G,A)$, sowie $B^n = \operatorname{im} d_n \simeq \operatorname{im} \partial_n = B^n_{\mathrm{h}}(G,A)$: daß beide Komplexe dieselben Kohomologiegruppen definieren, folgt *hieraus* aber wohl noch nicht.

Nachdem wir die Kohomologiegruppen $\mathrm{H}^n(G,A)$ für alle $n \geq 0$ konstruiert haben, weisen wir die Exaktheit der langen Kohomologiesequenz nach. Dazu gehen wir von einer exakten Sequenz (4.1) aus; damit ist auch

$$0 \longrightarrow \mathrm{K}^n(G,A) \longrightarrow \mathrm{K}^n(G,B) \longrightarrow \mathrm{K}^n(G,C) \longrightarrow 0 \qquad (4.2)$$

für alle $n \geq 0$ exakt: bis auf die Rechtsexaktheit des Funktors $\mathrm{K}^n(G,\,\cdot\,)$ ist dabei alles trivial. Sei also ein $h \in \mathrm{K}^n(G,C)$ gegeben. Wegen der Surjektivität von β gibt es zu jedem $s \in G^n$ ein $b \in B$ mit $h(s) = \beta(b)$. Damit können wir durch $g(s) = b$ eine Abbildung $g : G^n \longrightarrow B$ definieren (die natürlich von der Auswahl der b abhängt). Zu zeigen ist wegen $\beta \circ g = h$ nur, daß g stetig ist. Nun ist aber h nach Voraussetzung stetig, während β eine Abbildung zwischen diskreten Gruppen ist; damit muß dann auch g stetig sein.

Jetzt wenden wir das Schlangenlemma auf das aus (4.2) entstehende exakte kommutative Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{K}^n(A) & \longrightarrow & \mathrm{K}^n(B) & \longrightarrow & \mathrm{K}^n(C) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_{n+1}} & & \downarrow{\scriptstyle d_{n+1}} & & \downarrow{\scriptstyle d_{n+1}} & & \\
0 & \longrightarrow & \mathrm{K}^{n+1}(A) & \longrightarrow & \mathrm{K}^{n+1}(B) & \longrightarrow & \mathrm{K}^{n+1}(C) & \longrightarrow & 0
\end{array}$$

an (den Bezug auf G lassen wir weg, solange die Gruppe fest ist) und finden die exakte Sequenz

$$\begin{array}{ccccccc}
0 & \longrightarrow & C^n(A) & \longrightarrow & C^n(B) & \longrightarrow & C^n(C) \\
 & & & & & & \downarrow \\
0 & \longleftarrow & \frac{\mathrm{K}^{n+1}(C)}{\operatorname{im} d_{n+1}} & \longleftarrow & \frac{\mathrm{K}^{n+1}(B)}{\operatorname{im} d_{n+1}} & \longleftarrow & \frac{\mathrm{K}^{n+1}(A)}{\operatorname{im} d_{n+1}}
\end{array}$$

Ersetzen von n durch $n+1$ im oberen und durch $n-1$ im unteren Teil dieser Sequenz gibt uns ein exaktes kommutatives Diagramm

$$\begin{array}{ccccccccc}
 & & \frac{\mathrm{K}^n(A)}{\operatorname{im} d_n} & \longrightarrow & \frac{\mathrm{K}^n(B)}{\operatorname{im} d_n} & \longrightarrow & \frac{\mathrm{K}^n(C)}{\operatorname{im} d_n} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_{n+1}} & & \downarrow{\scriptstyle d_{n+1}} & & \downarrow{\scriptstyle d_{n+1}} & & \\
0 & \longrightarrow & C^{n+1}(A) & \longrightarrow & C^{n+1}(B) & \longrightarrow & C^{n+1}(C) & &
\end{array}$$

und das Schlangenlemma liefert

$$\begin{array}{ccccccc}
\mathrm{H}^n(G,A) & \xrightarrow{\alpha_n} & \mathrm{H}^n(G,B) & \xrightarrow{\beta_n} & \mathrm{H}^n(G,C) \\
 & & & & \downarrow{\scriptstyle \delta_n} \\
\mathrm{H}^{n+1}(G,C) & \xleftarrow{\beta_{n+1}} & \mathrm{H}^{n+1}(G,B) & \xleftarrow{\alpha_{n+1}} & \mathrm{H}^{n+1}(G,A)
\end{array}$$

Setzen wir diese Sequenzen für $n = 0, 1, 2, \ldots$ zusammen, so finden wir

Satz 4.1. *Sei G eine pro-endliche Gruppe und (4.1) eine kurze exakte Sequenz von diskreten G-Moduln. Dann existiert die lange exakte Kohomologiesequenz*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^0(G,A) & \longrightarrow & \mathrm{H}^0(G,B) & \longrightarrow & \mathrm{H}^0(G,C) \\ & & & & & & \downarrow \\ & & \mathrm{H}^1(G,C) & \longleftarrow & \mathrm{H}^1(G,B) & \longleftarrow & \mathrm{H}^1(G,A) \\ & & \downarrow & & & & \\ & & \mathrm{H}^2(G,A) & \longrightarrow & \mathrm{H}^2(G,B) & \longrightarrow & \mathrm{H}^2(G,C) \longrightarrow \ldots \end{array}$$

Faktorensysteme

Daß 1-Kozykel, also verschränkte Homomorphismen, eine Rolle in der Kummertheorie spielen, haben wir bereits gesehen. Die ersten Auftritte von 2-Kozykeln, auch Faktorensysteme genannt, stammen ebenfalls aus präkohomologischen Zeiten: einmal in der Theorie der Gruppenerweiterungen, zum andern in der Verkleidung als verschränkte Produkte in der Theorie zentral-einfacher Divisionsalgebren (Stichwort Brauergruppen).

Wir wissen, daß $\mathrm{H}^2(G,A) = C^2(G,A)/B^2(G,A)$ ist; hierbei besteht $C^2(G,A)$ aus stetigen Abbildungen $f : G \times G \longrightarrow A$ mit

$$\sigma_1 f(\sigma_2,\sigma_3) + f(\sigma_1,\sigma_2\sigma_3) = f(\sigma_1\sigma_2,\sigma_3) + f(\sigma_1,\sigma_2).$$

Weiter sind die zerfallenden Faktorensysteme solche $f : G \times G \longrightarrow A$, zu welchen es ein stetiges $g : G \longrightarrow A$ gibt mit

$$f(\sigma_1,\sigma_2) = \sigma_1 g(\sigma_2) - g(\sigma_1\sigma_2) + g(\sigma_1).$$

Am einfachsten lassen sich verschränkte Produkte erklären: diese tauchen in der Konstruktion gewisser K-Algebren A auf, also von K-Vektorräumen mit Ringstruktur. Die Ausgangsdaten sind eine endliche (!) galoissche Erweiterung L/K mit Galoisgruppe $G = \mathrm{Gal}\,(L/K)$, sowie ein 2-Kozykel $f \in C^2(G, L^\times)$. Zur Konstruktion der Algebra $A = (L/K, G, f)$ beginnen wir mit einem K-Vektorraum, und dieser ist bereits definiert durch die Angabe der Basis. Wir nehmen dazu für jedes $\sigma \in G$ ein Symbol x_σ und setzen $A = \bigoplus_{\sigma\in G} L x_\sigma$. Dies ist in offenkundiger Weise ein L-Vektorraum; die Multiplikation von Vektoren wird definiert durch K-lineare Fortsetzung der Regeln

$$\begin{aligned} x_\sigma x_\tau &= f(\sigma,\tau) x_{\sigma\tau}, \\ x_\sigma \alpha &= \alpha^\sigma x_\sigma \quad \text{für } \alpha \in L. \end{aligned}$$

Da G auf K trivial operiert, ist insbesondere $x_\sigma a = a x_\sigma$. Die Multiplikation zweier Elemente von A sieht damit so aus:

$$\begin{aligned}\sum_{\sigma\in G} a_\sigma x_\sigma \sum_{\tau\in G} a_\tau x_\tau &= \sum_{\sigma,\tau\in G} a_\sigma x_\sigma b_\tau x_\tau = \sum_{\sigma,\tau\in G} a_\sigma b_\tau^\sigma x_\sigma x_\tau \\ &= \sum_{\sigma,\tau\in G} a_\sigma b_\tau^\sigma f(\sigma,\tau) x_{\sigma\tau}.\end{aligned}$$

Nachzuprüfen ist selbstverständlich, daß diese Multiplikation assoziativ ist. In allen Gruppenstrukturen, die man mit Hilfe von 2-Kozykeln konstruiert, folgt die Assoziativität aus der Kozykelbedingung; insbesondere ist das hier so:

$$\begin{aligned}(x_\sigma x_\tau)x_\rho &= f(\sigma,\tau)x_{\sigma\tau}x_\rho = f(\sigma,\tau)f(\sigma\tau,\rho)x_{\sigma\tau\rho}, \quad \text{sowie} \\ x_\sigma(x_\tau x_\rho) &= x_\sigma f(\tau,\rho)x_{\tau\rho} = f(\tau,\rho)^\sigma x_\sigma x_{\tau\rho} = f(\tau,\rho)^\sigma f(\sigma,\tau\rho)x_{\sigma\tau\rho}.\end{aligned}$$

Damit haben wir aus L/K, der Galoisgruppe $G = \mathrm{Gal}\,(L/K)$ und dem 2-Kozykel $f \in C^2(G, L^\times)$ eine K-Algebra $A = (L/K, G, f)$ konstruiert, die man auch ein *verschränktes Produkt* nennt. Eine leichte Übung zeigt, daß die Isomorphieklasse von A nur von der Klasse von f in $\mathrm{H}^2(G, L^\times)$ abhängt! Insbesondere haben wir eine Abbildung aus der Gruppe $\mathrm{H}^2(G, L^\times)$ in Isomorphieklassen von Algebren. Tatsächlich kann man auch letztere zu einer Gruppe machen (die Komposition wird durch das Tensorprodukt induziert, allerdings muß man von den Isomorphieklassen noch zu gröberen Äquivalenzklassen übergehen), und dann wird aus dieser Abbildung ein injektiver Homomorphismus; das Bild von $\mathrm{H}^2(G, L^\times)$ in dieser Gruppe nennt man die Brauergruppe $\mathrm{Br}(L/K)$. Läßt man L die endlichen normalen Erweiterungen durchlaufen, erhält man ein projektives System, dessen Limes $\mathrm{Br}(K) \simeq \mathrm{H}^2(\mathrm{Gal}\,(\overline{K}/K), \overline{K})$ die Brauergruppe von K heißt. Diese Brauergruppe ist eine wichtige Invariante des Körpers K: die Aussage $\mathrm{Br}(K) = 0$ für endliche Körper ist beispielsweise äquivalent zum Satz von Wedderburn, wonach jede endliche Divisionsalgebra bereits ein Körper ist. Das Ergebnis $\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$ für endliche Erweiterungen K von $\mathbb{Q}_p$ dagegen ist im wesentlichen der Kern der lokalen Klassenkörpertheorie, und die Bestimmung der Brauergruppe von Zahlkörpern enthält einen Großteil der globalen Klassenkörpertheorie in algebrentheoretischem Gewand.

Gruppenerweiterungen

Sei A eine endliche abelsche Gruppe, G pro-endlich. Eine kurze exakte Sequenz

$$1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$$

heißt Gruppenerweiterung von G mit A. Zwei solche Erweiterungen nennt man äquivalent, wenn es ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \Gamma & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & A & \longrightarrow & \Gamma' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

gibt; nach dem Schlangenlemma impliziert dies, daß ϕ ein Isomorphismus ist – allerdings ist die Existenz eines Isomorphismus $\phi : \Gamma \longrightarrow \Gamma'$ nicht hinreichend für die Äquivalenz der beiden Gruppenerweiterungen.

Eine Gruppenerweiterung wird durch zwei Invarianten beschrieben:

- einem Homomorphismus $\Phi : G \longrightarrow \mathrm{Aut}\,(A)$;
- einem Faktorensystem $f \in \mathrm{H}^2(G, A)$.

Γ operiert nämlich auf dem Normalteiler A per Konjugation, und da A abelsch ist, operiert A trivial auf sich, d.h. wir erhalten eine Operation von $G = \Gamma/A$ auf A, mit anderen Worten einen Homomorphismus $\Phi : G \longrightarrow \mathrm{Aut}\,(A)$. Explizit ist diese Operation gegeben durch $\sigma \longmapsto (a \longmapsto u_\sigma a u_\sigma^{-1})$. Hier ist $u : G \longrightarrow \Gamma$ ein stetiger Schnitt, also eine stetige Abbildung, die jedem $\sigma \in G$ ein Urbild $u_\sigma \in \Gamma$ zuordnet (daß man dies auf stetige Art und Weise machen kann, ist im Falle pro-endlicher Gruppen ein zu beweisender Satz!).

Wir können nun jedes Element $\gamma \in \Gamma$ in der Form $\gamma = a u_\sigma$ mit $\sigma \in G$ und $a \in A$ schreiben. Zu jedem Paar $\sigma, \tau \in G$ gibt es dann ein Element $a_{\sigma,\tau} \in A$ mit $u_\sigma u_\tau = a_{\sigma,\tau} u_{\sigma\tau}$. Benutzt man die Assoziativität von Γ, so stellt man fest, daß die Abbildung $G \times G \longrightarrow A : (\sigma, \tau) \longmapsto a_{\sigma,\tau}$ ein Faktorensystem ist.

Sind umgekehrt eine Gruppe G, ein G-Modul A und ein Faktorensystem $a \in \mathrm{H}^2(G, A)$ gegeben, so kann man das kartesische Produkt $A \times G$ zu einer Gruppe machen, indem man $(a, \sigma) * (b, \tau) = (ab^\sigma a_{\sigma,\tau}, \sigma\tau)$ setzt. Damit ist klar, daß das triviale Faktorensystem $a_{\sigma,\tau} = 1$ auf das bekannte semidirekte Produkt führt; ist darüberhinaus A ein trivialer G-Modul, erhält man das direkte Produkt von G und A.

Unterscheiden sich zwei Faktorensysteme um einen 2-Korand, so sind die entsprechenden Gruppenerweiterungen äquivalent (und umgekehrt). Wir haben also eine Bijektion zwischen den Elementen von $\mathrm{H}^2(G, A)$ und den Äquivalenzklassen von Gruppenerweiterungen von G mit A.

4.2 Inflation und Restriktion

Sei H abgeschlossene Untergruppe der pro-endlichen Gruppe G und A ein diskreter G-Modul. Dann ist A erst recht ein diskreter H-Modul, und dies liefert uns einen Homomorphismus $\mathrm{res} : \mathrm{H}^n(G, A) \longrightarrow \mathrm{H}^n(H, A)$ wie folgt: einem $x \in C^n(G, A)$, das durch eine Abbildung $f : G^n \longrightarrow A$ repräsentiert ist, ordnen wir die Klasse der Einschränkung von f auf $H^n \longrightarrow A$ zu. Diese Einschränkung ist natürlich ebenfalls wieder stetig und verträgt sich mit Randoperatoren, liefert also in der Tat einen Homomorphismus $\mathrm{res} : \mathrm{H}^n(G, A) \longrightarrow \mathrm{H}^n(H, A)$.

Ist andererseits N ein abgeschlossener Normalteiler in G, so operiert G/N stetig auf dem Fixmodul A^N. Einem Element $x \in C^q(G/N, A^N)$ können wir ein $x' = \inf_N^G x \in C^q(G, A)$ zuordnen, indem wir $x'(\sigma_1, \ldots, \sigma_n) = x(\sigma_1 N, \ldots, \sigma_n N)$

setzen. Weil dabei Coränder auf Coränder übergehen, induziert dies einen Homomorphismus $\inf_N^G : \mathrm{H}^q(G/N, A^N) \longrightarrow \mathrm{H}^q(G, A)$, die Inflation.

Restriktion und Inflation sind Beispiele für eine Konstruktion von Homomorphismen zwischen Kohomologiegruppen, die im nächsten Abschnitt genauer untersucht wird.

Kompatible Homomorphismen

Ist $f : A \longrightarrow B$ ein G-Homomorphismus diskreter G-Moduln, so wird dadurch ein Homomorphismus $f^* : \mathrm{H}^q(G, A) \longrightarrow \mathrm{H}^q(G, B)$ induziert: das folgt bereits aus entsprechenden funktoriellen Eigenschaften des Schlangenlemmas und der Tatsache, daß wir die Kohomologiegruppen mit diesem konstruiert haben. Dies läßt sich nun wie folgt verallgemeinern: sind G und G' pro-endliche Gruppen, welche auf den diskreten Moduln A bzw. A' stetig operieren, und sind ein stetiger Homomorphismus $g : G \longrightarrow G'$ sowie ein Homomorphismus $f : A' \longrightarrow A$ gegeben, so heißen f und g kompatibel, wenn $f(g(\sigma)a') = \sigma f(a')$ für alle $\sigma \in G$ und alle $a' \in A'$ gilt. Man kann die letzte Bedingung auch so ausdrücken: macht man A' zu einem G-Modul via $\sigma(a') = g(\sigma)(a')$, so soll der Homomorphismus f ein G-Homomorphismus sein.

Ein kompatibles Paar (g, f) induziert einen Homomorphismus zwischen den Gruppen $(g, f) : K^q(G', A') \longrightarrow K^q(G, A)$, der durch Komposition

$$G^q \xrightarrow[g]{} G'^q \xrightarrow[x']{} A' \xrightarrow[f]{} A$$

definiert wird, d.h. durch $(g, f)x'(\sigma_1, \ldots, \sigma_q) = f(x'(g(\sigma_1), \ldots, g(\sigma_q)))$. Jetzt gilt es nachzuweisen, daß (g, f) mit den Korandoperatoren kommutiert:

$$\begin{array}{ccc} K^q(G', A') & \xrightarrow[d_{q+1}]{} & K^{q+1}(G', A') \\ \downarrow{\scriptstyle (g,f)} & & \downarrow{\scriptstyle (g,f)} \\ K^q(G, A) & \xrightarrow[d_{q+1}]{} & K^{q+1}(G, A) \end{array}$$

Sei dazu ein $x' \in K^q(G', A')$ gegeben. Dann ist

$$\begin{aligned} \delta_{q+1}(g, f)x'(\sigma_1, \ldots, \sigma_{q+1}) &= \sigma_1(g, f)x'(\sigma_2, \ldots, \sigma_{q+1}) \\ &\quad + \sum_{i=1}^{q}(-1)^i(g, f)x'(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{q+1}) \\ &\quad + (-1)^{q+1}(g, f)x'(\sigma_1, \ldots, \sigma_q) \\ &= \sigma_1 f x'(g(\sigma_2), \ldots, g(\sigma_{q+1})) \\ &\quad + \sum_{i=1}^{q}(-1)^i f x'(g(\sigma_1), \ldots, g(\sigma_i\sigma_{i+1}), \ldots, g(\sigma_{q+1})) \\ &\quad + (-1)^{q+1} f x'(g(\sigma_1), \ldots, g(\sigma_q)), \end{aligned}$$

sowie andererseits

$$\begin{aligned}(g,f)\delta_{q+1}x'(\sigma_1,\dots,\sigma_{q+1}) &= f\delta_{q+1}x'(g(\sigma_1),\dots,g(\sigma_{q+1}))\\ &= f\Big[g(\sigma_1)x'(g(\sigma_2),\dots,g(\sigma_{q+1}))\\ &\quad+\sum_{i=1}^{q}(-1)^i x'(g(\sigma_1),\dots,g(\sigma_i)g(\sigma_{i+1}),\dots,g(\sigma_{q+1}))\\ &\quad+(-1)^{q+1}x'(g(\sigma_1),\dots,g(\sigma_q))\Big],\end{aligned}$$

und wenn man beachtet, daß f und g kompatibel und Homomorphismen sind, so sieht man, daß beide Ausdrücke übereinstimmen. Damit können wir (g,f) auf die Kohomologiegruppen fortsetzen und erhalten Homomorphismen

$$(g,f):\mathrm{H}^q(G',A')\longrightarrow\mathrm{H}^q(G,A).$$

In der Tat induziert (g,f) einen Homomorphismus $C^q(G',A')\longrightarrow K^q(G,A)$; wegen $d_{q+1}(g,f)=(g,f)d_{q+1}$ liegt das Bild aber sogar in $C^q(G,A)$. Weil aus demselben Grund Coränder in Coränder übergehen, liefert (g,f) wie behauptet einen Homomorphismus auf den Kohomologiegruppen.

Proposition 4.2. *Sind G_i $(i=1,2,3)$ pro-endliche Gruppen, A_i $(i=1,2,3)$ diskrete G_i-Moduln, und seien stetige Homomorphismen $g_1:G_1\longrightarrow G_2$, $g_2:G_2\longrightarrow G_3$, $f_1:A_2\longrightarrow A_1$ und $f_2:A_3\longrightarrow A_2$ gegeben. Sind (g_1,f_1) und (g_2,f_2) kompatibel, so auch $(g_2\circ g_1, f_1\circ f_2)$, und es gilt $(g_1,f_1)\circ(g_2,f_2)=(g_2\circ g_1, f_1\circ f_2)$.*

Die letzte Behauptung folgt direkt aus der Betrachtung der entsprechenden Diagramme.

Beispiel 1. Sei H abgeschlossene Untergruppe von G, A ein diskreter G-Modul, $g:H\longrightarrow G$ die Inklusion, und $f=\mathrm{id}$ die Identität auf A. Dann sind g und f kompatibel wegen $g(\sigma)a=\sigma(a)$ für alle $\sigma\in H$. Der von (g,f) induzierte Homomorphismus $\mathrm{H}^q(G,A)\longrightarrow\mathrm{H}^q(H,A)$ ist nichts anderes als die Restriktion. Weiter folgt für abgeschlossene Untergruppen $U\subseteq V\subseteq G$ die Eigenschaft

$$\mathrm{res}^V_U\circ\mathrm{res}^G_V=\mathrm{res}^G_U$$

direkt aus Proposition 4.2.

Beispiel 2. Sei N ein abgeschlossener Normalteiler einer pro-endlichen Gruppe G, $g:G\longrightarrow G/N$ die kanonische Projektion und $f:A^N\longrightarrow A$ die Injektion. Dann sind g und f kompatibel, und es gilt $(g,f)=\mathrm{inf}^G_N$.

Satz 4.3. *Sei N ein abgeschlossener Normalteiler der pro-endlichen Gruppe G, und sei A ein diskreter G-Modul. Dann ist die Inflations-Restriktions-Sequenz*

$$0\longrightarrow\mathrm{H}^1(G/N,A^N)\xrightarrow{\mathrm{inf}}\mathrm{H}^1(G,A)\xrightarrow{\mathrm{res}}\mathrm{H}^1(N,A)$$

exakt.

Beweis. Wir haben zu zeigen, daß inf injektiv ist. Sei dazu $x : G/N \longrightarrow A^N$ ein stetiger 1-Cozykel. Wenden wir die Inflation auf x an, so haben wir das Bild $x' = \inf x$ als 1-Cozykel $G \longrightarrow A$ aufzufassen via $G \longrightarrow G/N \longrightarrow A^N \longrightarrow A$. Falls x' Corand ist, so gibt es ein $a \in A$ mit $x'(\sigma) = \sigma a - a$. Nun ist x' konstant auf den Nebenklassen von G/N, d.h.es gilt $\sigma a - a = \sigma\tau a - a$ für alle $\tau \in N$. Dies impliziert $a = \tau a$ für alle $\tau \in N$, also $a \in A^N$. Damit ist $x(\sigma N) = \sigma N a - a$ ein 1-Corand.

Der zweite Punkt, der zu zeigen ist, ist $\operatorname{im}\inf = \ker\operatorname{res}$. Wir beginnen mit "$\subseteq$": ist $x : G/N \longrightarrow A^N$ ein 1-Cozykel, so ist $\inf_N^G x(\sigma) = x(\sigma N)$ und damit $\operatorname{res}_N^G \circ \inf_N^G x(\tau) = x(N)$ für $\tau \in N$. Da N das neutrale Element von G/N ist und für 1-Cozykel die Gleichung $x(0) = 0$ besteht, folgt in der Tat $\operatorname{res}_N^G \circ \inf_N^G = 0$ und damit die Behauptung.

Für die Umkehrrichtung sei $y : G \longrightarrow A$ ein 1-Cozykel, dessen Einschränkung auf N ein Corand ist. Dann gibt es ein $a \in A$ mit $y(\tau) = \tau a - a$. Indem wir von y den Corand $\sigma \longmapsto \sigma a - a$ subtrahieren, erhalten wir einen 1-Cozykel, der in derselben Klasse wie y liegt und dessen Einschränkung auf N verschwindet. Bezeichnen wir diesen Cozykel wieder mit y, so zeigt $y(\sigma\tau) = y(\sigma) + \sigma y(\tau) = y(\sigma)$ für alle $\tau \in N$, daß y auf den Nebenklassen von G/N konstant ist. Weiter ist $y(\sigma\tau) = \sigma y(\tau)$ für alle $\sigma \in N$ und $\tau \in G$, und wegen $\sigma\tau = \tau\sigma'$ für ein $\sigma' \in N$ gilt $\sigma y(\tau) = y(\sigma\tau) = y(\tau\sigma') = y(\tau)$, d.h. im $y \in A^N$. Also ist y die Inflation eines 1-Cozykels $G/N \longrightarrow A^N$. □

Man kann die Kohomologiegruppen $\mathrm{H}^q(N, A)$ zu einem G-Modul machen und zeigen, daß N dabei trivial auf $\mathrm{H}^q(N, A)$ operiert; damit wird $\mathrm{H}^q(N, A)$ zu einem G/N-Modul, und es ist nicht schwer zu zeigen, daß das Bild der Restriktion sogar in $\mathrm{H}^q(N, A)^{G/N}$ landet. Die Inflations-Restriktions-Sequenz

$$0 \longrightarrow \mathrm{H}^1(G/N, A^N) \xrightarrow{\inf} \mathrm{H}^1(G, A) \xrightarrow{\operatorname{res}} \mathrm{H}^1(N, A)^{G/N}$$

ist dann der Anfang der Hochschild-Serre-Spektralsequenz

$$0 \longrightarrow \mathrm{H}^1(G/N, A^N) \xrightarrow{\inf} \mathrm{H}^1(G, A) \xrightarrow{\operatorname{res}} \mathrm{H}^1(N, A)^{G/N} \xrightarrow{\operatorname{tra}} \mathrm{H}^2(G/N, A) \xrightarrow{\inf} \mathrm{H}^2(G, A),$$

wobei die Transgression tra auf direktem Weg nur ziemlich umständlich definiert werden kann (sh. z.B. die früher zitierten Bücher von Koch und Poitou). Der "richtige" Beweis benutzt Spektralsequenzen (die findet man z.B. in Ribet oder Shatz).

4.3 Induzierte Moduln

Kohomologisch betrachtet sind induzierte Moduln ausgesprochen hübsche Objekte: die Tatsache, daß deren Kohomologiegruppen H^q für alle $q \geq 1$ trivial sind, kann man dazu verwenden, die komplette Theorie auf die Gruppe

$\mathrm{H}^0(G,A)$ zurückzuführen. Die zugrundegelegte Technik hört auf den Namen "Dimensionsverschiebung" und ist das zentrale Hilfsmittel in Kochs Buch über die Galoissche Theorie der p-Erweiterungen.

Sei G pro-endliche Gruppe, H eine abgeschlossene Untergruppe, und A ein diskreter H-Modul. Wir betrachten die Menge

$$\mathrm{ind}_H^G(A) = \{f : G \longrightarrow A \text{ stetig, und } f(hg) = h \cdot f(g) \text{ für alle } h \in H\}.$$

Diese ist in offensichtlicher Weise eine additive Gruppe.

Jetzt definieren wir $(\tau f)(\sigma) = f(\sigma\tau)$ für $\tau \in G$. Dies definiert zuerst einmal eine Operation von G auf $\mathrm{ind}_H^G(A)$: dazu ist zu zeigen, daß $(\rho\tau)f = \rho(\tau f)$ für $\rho, \tau \in G$ gilt. Nun ist aber $[(\rho\tau)f](\sigma) = f(\sigma\rho\tau)$, sowie $[\rho(\tau f)](\sigma) = (\tau f)(\sigma\rho) = f(\sigma\rho\tau)$.

Mit f ist natürlich auch τf stetig, und wir behaupten, daß $B = \mathrm{ind}_H^G(A)$ dadurch zu einem diskreten G-Modul wird. Dazu müssen wir zeigen, daß es zu jedem $f \in B$ einen offenen Normalteiler U von G gibt mit $f \in B^U$. Dazu beachten wir, daß zu f einen Normalteiler N von G gibt, sodaß f auf den Nebenklassen von G/N konstant ist. Damit ist dann $f(\sigma) = f(\sigma\tau) = (\tau f)(\sigma)$ für alle $\tau \in N$, d.h. mit $U = N$ ist $f \in B^U$.

Damit haben wir zu jeder abgeschlossenen Untergruppe H von G und jedem diskreten H-Modul A einen diskreten G-Modul $\mathrm{ind}_H^G(A)$ konstruiert. Im Spezialfall $H = 1$ (d.h. wenn A eine beliebige abelsche Gruppe ist) schreiben wir $M_G(A) = \mathrm{ind}_1^G(A)$ und nennen $M_G(A)$ den induzierten Modul.

Jeder G-Modul A ist auch H-Modul, und dieser kann wie folgt als Untermodul von $\mathrm{ind}_H^G(A)$ aufgefaßt werden: die Abbildung $A \longrightarrow \mathrm{ind}_H^G(A) : a \longmapsto f_a$ mit $f_a(\sigma) = \sigma(a)$ für $\sigma \in G$ (dazu muß A ein G-Modul sein) ist nämlich offensichtlich injektiv, es ist $f_a(\tau\sigma) = \tau(f_a(\sigma))$ für alle $\tau \in H$, und es gilt $f_{\tau a} = \tau f_a$ für alle $\tau \in G$: in der Tat ist $f_{\tau a}(\sigma) = \sigma\tau(a)$, sowie $\tau f_a(\sigma) = f_a(\sigma\tau) = \sigma\tau(a)$. Damit haben wir insbesondere für jeden diskreten G-Modul A eine exakte Sequenz

$$0 \longrightarrow A \longrightarrow M_G(A) \longrightarrow C \longrightarrow 0,$$

wo C den Quotientenmodul $M_G(A)/A$ bezeichnet.

Induzierte Moduln haben triviale Kohomologie

Sei G pro-endlich, A eine abelsche Gruppe, und $B = \mathrm{ind}_1^G(A)$ der induzierte G-Modul. Wir wollen zeigen, daß $\mathrm{H}^q(G,B) = 0$ für alle $q \geq 1$ gilt (offenbar ist $\mathrm{H}^0(G,B) = (\mathrm{ind}_1^G(B))^G \simeq A$, wobei A als trivialer G-Modul aufzufassen ist: man stellt nämlich sofort fest, daß $(\mathrm{ind}_1^G(B))^G$ nur aus den konstanten Funktionen besteht, und diese können wie üblich mit ihren Bildern identifiziert werden). Dazu betrachten wir $\mathrm{Abb}_c(G^n, B)$, also die Gruppe der stetigen Abbildungen $G^n \longrightarrow B$, und stellen fest, daß wir $\mathrm{Abb}_c(G^q, B)$ mit $\mathrm{Abb}_c(G^{q+1}, A)$ identifizieren können: dazu fassen wir ein stetiges

$$\phi : G^q \longrightarrow B = \mathrm{Abb}\,(G, A) : (x_1, \ldots, x_q) \longmapsto \psi$$

als stetige Abbildung

$$\Phi : G^{q+1} \longrightarrow A : (x_1, \ldots, x_q|x) \longmapsto \psi(x)$$

auf: die letzte Koordinate von G^{q+1} gibt also an, an welcher Stelle ψ, das Bild der ersten q Koordinaten, ausgewertet werden soll. Dies erlaubt uns, die Gruppe der q-Koketten als

$$K^q(G,B) = \{\Phi : G^{q+1} \longrightarrow A \text{ stetig}\}$$

aufzufassen.

Jetzt definieren wir für jedes $\sigma \in G$ einen Homomorphismus

$$\begin{aligned} s_q(\sigma) :& K^q(G,B) \longrightarrow K^{q-1}(G,B) : \\ & [s_q(\sigma)\Phi](x_1, \ldots, x_{q-1}|x) \;=\; \Phi(\sigma^{-1}x, x_1, \ldots, x_{q-1}|\sigma). \end{aligned}$$

Damit gilt dann

$$\partial_q s_q(\sigma)\Phi + s_{q+1}(\sigma)\partial_{q+1}\Phi = \Phi.$$

Hier ist das entsprechende Diagramm:

$$\begin{array}{ccc} K^q(G,B) & \xrightarrow{s_q(\sigma)} & K^{q-1}(G,B) \\ \downarrow{\scriptstyle \partial_{q+1}} & & \downarrow{\scriptstyle \partial_q} \\ K^{q+1}(G,B) & \xrightarrow{s_{q+1}(\sigma)} & K^q(G,B) \end{array}$$

Behauptet ist also: geht man in beiden Richtungen von links oben nach rechts unten und addiert die Ergebnisse auf, so erhält man das Ausgangselement zurück.

Wir finden nun in der Tat

$$\begin{aligned} [\partial_q s_q(\sigma)\Phi](x_1, \ldots, x_q|x) &= x_1 s_q(\sigma)\Phi(x_2, \ldots, x_q|x) \\ &+ \sum_{i=1}^{q-1}(-1)^i s_q(\sigma)\Phi(x_1, \ldots, x_i x_{i+1}, \ldots, x_q|x) \\ &+ (-1)^q s_q(\sigma)\Phi(x_1, \ldots, x_{q-1}|x); \end{aligned}$$

beachtet man, auf welche Art wir $M_G(A)$ zu einem G-Modul gemacht haben, so folgt $x_1 s_q(\sigma)\Phi(x_2, \ldots, x_q|x) = s_q(\sigma)\Phi(x_2, \ldots, x_q|xx_1)$, also weiter

$$\begin{aligned} [\partial_q s_q(\sigma)\Phi](x_1, \ldots, x_q|x) &= \Phi(\sigma^{-1}xx_1, x_2, \ldots, x_q|\sigma) \\ &+ \sum_{i=1}^{q-1}(-1)^i \Phi(\sigma^{-1}x, x_1, \ldots, x_i x_{i+1}, \ldots, x_q|\sigma) \\ &+ (-1)^q \Phi(\sigma^{-1}x, x_1, \ldots, x_{q-1}|\sigma), \end{aligned}$$

sowie andererseits

$$\begin{aligned} s_{q+1}(\sigma)\partial_{q+1}\Phi(x_1,\dots,x_q|x) &= \partial_{q+1}\Phi(\sigma^{-1}x,x_1,\dots,x_q|\sigma) \\ &= \sigma^{-1}x\Phi(x_1,\dots,x_q|\sigma) - \Phi(\sigma^{-1}xx_1,x_2,\dots,x_q|\sigma) \\ &+ \sum_{i=1}^{q-1}(-1)^{i+1}\Phi(\sigma^{-1}x,x_1,\dots,x_ix_{i+1},\dots,x_q|\sigma) \\ &+ (-1)^{q+1}\Phi(\sigma^{-1}x,x_1,\dots,x_{q-1}|\sigma). \end{aligned}$$

Addieren liefert unter der Beachtung der Operation von G auf B

$$\begin{aligned} [\partial_q s_q(\sigma)\Phi + s_{q+1}(\sigma)\partial_{q+1}\Phi](x_1,\dots,x_q|x) &= \sigma^{-1}x\Phi(x_1,\dots,x_q|\sigma) \\ &= \Phi(x_1,\dots,x_q|x). \end{aligned}$$

Jetzt bekommen wir

Satz 4.4. *Für alle $q \geq 1$ ist $\mathrm{H}^q(G, M_G(A)) = 0$.*

Beweis. Sei $y \in K^q(G, M_G(A))$ ein q-Kozykel, also $\partial_{q+1}y = 0$. Wir haben zu zeigen, daß y bereits ein q-Korand ist, also ein $x \in K^{q-1}(G, M_G(A))$ existiert mit $y = \partial_q x$. Wegen $\Phi = \partial_q s_q(\sigma)\Phi + s_{q+1}(\sigma)\partial_{q+1}\Phi = \partial_q s_q(\sigma)\Phi$ für irgendein $\sigma \in G$ ist dies aber klar. □

Dieses Ergebnis ist übrigens ist ein Spezialfall von

Satz 4.5 (Lemma von Shapiro). *Ist H eine abgeschlossene Untergruppe der pro-endlichen Gruppe G und A ein diskreter G-Modul, dann gilt für alle $q \geq 0$*

$$\mathrm{H}^q(G, \mathrm{ind}_H^G(A)) \simeq \mathrm{H}^q(H, A).$$

Der Beweis beruht auf Dimensionsverschiebung (sh. Koch, Kap. 3).

Funktorialitäten

In diesem Abschnitt wird gezeigt, daß ind_H^G ein exakter Funktor aus der Kategorie der diskreten H-Moduln in die der diskreten G-Moduln ist, und daß mit (I, G_i, A_i) auch $(I, G_i, M_{G_i}(A_i))$ ein induktives System ist. Diese Ergebnisse werden im folgenden nicht benötigt.

Die Konstruktion der induzierten Moduln ist (selbstverständlich) funktoriell: sind $A, B \in \mathrm{Mod}\,(H)$, und ist $f : A \longrightarrow B$ ein H-Homomorphismus, so induziert f einen Homomorphismus $f_* : \mathrm{ind}_H^G(A) \longrightarrow \mathrm{ind}_H^G(B)$, welcher ein $\phi \in \mathrm{ind}_H^G(A)$ auf das Element $f \circ \phi \in \mathrm{ind}_H^G(B)$ abbildet. Damit wird ind_H^G zu einem exakten Funktor der Kategorie der diskreten H-Moduln in die der diskreten G-Moduln:

Proposition 4.6. *Sei G pro-endlich, $H \leq G$ eine abgeschlossene Untergruppe von G, weiter $A, B, C \in \mathrm{Mod}\,(G)$. Ist die Sequenz*

$$0 \longrightarrow A \xrightarrow{\ i\ } B \xrightarrow{\ j\ } C \longrightarrow 0$$

exakt, dann auch

$$0 \longrightarrow \mathrm{ind}_H^G(A) \xrightarrow{i_*} \mathrm{ind}_H^G(B) \xrightarrow{j_*} \mathrm{ind}_H^G(C) \longrightarrow 0.$$

Beweis. Sei $\phi \in \mathrm{ind}_H^G(A)$ und $i(\phi) = 0$. Da i injektiv ist, muß $\phi = 0$ sein. Also ist i_* injektiv.

Ist $\phi \in \mathrm{ind}_H^G(A)$, so gilt $j \circ i \circ \phi = 0$, folglich $j_* \circ i_* = 0$. Ist umgekehrt $\psi \in \mathrm{ind}_H^G(B)$ und $j \circ \psi = 0$, so existiert zu jedem $\sigma \in G$ ein $a \in A$ mit $\psi(\sigma) = i(a)$. Definiere eine Abbildung $\phi : G \longrightarrow A$ durch $\phi(\sigma) = a$; wegen der Injektivität von i ist ϕ wohldefiniert. Weiter ist $\phi \in \mathrm{ind}_H^G(A)$, da erstens wegen $\psi(hg) = h\psi(g) = hi(a) = i(ha)$ sicher $\phi(hg) = h\phi(g)$ ist, und da zweitens ϕ stetig ist, weil $i \circ \phi = \psi$ stetig ist. Dies zeigt Exaktheit an der Stelle $\mathrm{ind}_H^G(B)$.

Schließlich ist noch die Surjektivität von j_* zu beweisen. Sei dazu $\psi \in \mathrm{ind}_H^G(C)$; da ψ für einen geeigneten offenen Normalteiler N auf Nebenklassen gN konstant ist, nimmt ψ nur endlich viele Werte an, sagen wir $\psi(G) = \{c_1, \ldots, c_n\}$. Zu jedem c_i können wir ein $b_i \in B$ finden mit $j(b_i) = c_i$. Für jedes i betrachten wir nun die Untergruppe $V_i = \{h \in H : hb_i = b_i\}$ von H; als Stabilisator von b_i ist V_i offen in H und es gibt somit einen offenen Normalteiler U_1 von G mit $U_1 \cap H \subseteq V_i$ für die endlich vielen i. Wegen der Stetigkeit von ψ gibt es einen zweiten offenen Normalteiler U_2 von G mit $f(gU_2) = f(g)$. Sei nun $U = U_1 \cap U_2$: dann ist mit $(G : U)$ erst recht $t = (G : HU)$ endlich. Seien $g_1, \ldots, g_t$ Vertreter der Nebenklassen von G/HU. Zu jedem g_i wählen wir aus der Menge $\{b_1, \ldots, b_n\}$ ein β_i aus mit $f(\beta_i) = f(g_i)$ und definieren eine Abbildung $\phi : G \longrightarrow B$, indem wir $g = hug_i$ schreiben und $\phi(g) = h\beta_i$ setzen. Dann ist ϕ wohldefiniert und stetig: ist nämlich $u \in U$ und $g \in G$, so ist $\phi(ug) = \phi(g)$, also ϕ konstant auf Nebenklassen von G/U. Weiter ist noch $\phi(hg) = h\phi(g)$ für $h \in H$ und $g \in G$: mit $g = h'ug_i$ ist nämlich $\phi(hg) = \phi(hh'ug_i) = hh'\beta_i = h\phi(g)$. Schließlich gilt natürlich auch $f \circ \phi = \psi$, und wir haben fertig. □

Sind $U \leq H$ abgeschlossene Untergruppen einer pro-endlichen Gruppe G und ist A ein diskreter U-Modul, so überzeugt man sich auch leicht davon, daß $\mathrm{ind}_H^G \circ \mathrm{ind}_U^H = \mathrm{ind}_U^G$ gilt.

4.4 Direkte Limites von Kohomologiegruppen

Wir beginnen mit einer Erinnerung an direkte Systeme: ist I gerichtete Menge, sind A_i abelsche Gruppen, und sind Homomorphismen $\lambda_{ji} : A_i \longrightarrow A_j$ gegeben, so heißt $(I, \leq, \{A_i\}, \lambda_{ji})$ ein direktes System, wenn $\lambda_{ii} = \mathrm{id}$ und $\lambda_{ji} \circ \lambda_{kj} = \lambda_{ki}$ ist für alle $i, j, k \in I$ mit $i \leq j \leq k$. Sei A die disjunkte Vereinigung der A_i und $a, b \in A$; dann setzen wir $a \sim b$, falls $a \in A_i$, $b \in A_j$ und es ein $k \in I$ gibt mit $\lambda_{ki}a = \lambda_{kj}b$. Die Menge der Äquivalenzklassen $A/\sim$ nennt man den direkten Limes und schreibt $A/\sim = \varinjlim A_i$. Diesem Objekt kann man

eine Gruppenstruktur verpassen: sind a und b die Klassen von a_i und b_j, so soll $a+b$ die Äquivalenzklasse von $\lambda_{ki}a_i + \lambda_{kj}b_j$ sein. Das ganze ist, wie man leicht sieht, wohldefiniert.

Sei I eine gerichtete Indexmenge, $(\{G_i\}, \pi_{ji})$ ein projektives System endlicher Gruppen, $(\{A_i\}, \lambda_{ji})$ ein direktes System abelscher Gruppen, wobei jedes A_i ein G_i-Modul sein soll. Außerdem sollen $\pi_{ji} : G_j \longrightarrow G_i$ und $\lambda_{ji} : A_i \longrightarrow A_j$ kompatibel sein. Mit $G = \varprojlim G_i$ und $A = \varinjlim A_i$ kann man A so zu einem G-Modul machen, daß die kanonischen Abbildungen $A_i \longrightarrow A$ und $G \longrightarrow G_i$ kompatibel sind: ist nämlich $g = (g_i) \in G$ und $a \in A$, wobei a das Bild von $a_i \in A_i$ ist, so muß man ga als das Bild von $g_i a_i$ definieren und nachrechnen, daß dies wohldefiniert ist und die kanonischen Homomorphismen $\lambda_i : A_i \longrightarrow A$ und $\pi_i : G \longrightarrow G_i$ kompatibel sind.

Sind nun weiter alle A_i diskrete G_i-Moduln, so ist A ein diskreter G-Modul: zu zeigen ist, daß die Abbildung $G \times \{a\} \longrightarrow A : (\sigma, a) \longmapsto \sigma(a)$ stetig ist. Mit $a = \overline{a_i}$ für ein $a_i \in A_i$ ist aber $\sigma(a) = \pi_j(\sigma)(a_i)$, und die Operation von G_i auf A_i sowie die anschließende Einbettung $\lambda_i : A_i \longrightarrow A$ sind stetig.

Wir nennen nun $(I, [G_i, A_i], (\pi_{ji}, \lambda_{ji}))$ ein induktives System, wenn (I, G_i, π_{ji}) projektives System (pro-) endlicher Gruppen, (I, A_i, λ_{ji}) direktes System diskreter G_i-Moduln, und die auftretenden Abbildungen verträglich sind. Im Spezialfall $G_i = 1$ erhält man direkte Systeme abelscher Gruppen.

Proposition 4.7. *Sind (A_i, λ_{ji}) und (B_i, μ_{ji}) direkte Systeme abelscher Gruppen und sind die $\phi_i : A_i \longrightarrow B_i$ verträgliche Homomorphismen, dann induzieren diese einen Homomorphismus $\phi : \varinjlim A_i \longrightarrow \varinjlim B_i$. Sind alle ϕ_i injektiv (surjektiv), dann gilt dies auch für ϕ; darüberhinaus ist $\varinjlim$ ein exakter Funktor in der Kategorie der direkten Systeme abelscher Gruppen.*

Beweis. Sei $a \in A = \varinjlim A_i$ und $a = \overline{a_i}$ mit $a_i \in A_i$. Dann definieren wir $\phi(a) = \mu_i(\phi_i(a_i))$, wo $\mu_i : B_i \longrightarrow A$ wie üblich erklärt ist. Ist $a_j \in A_j$ ein anderer Repräsentant der Klasse a, so gibt es ein $k \geq i, j$ mit $\lambda_{ki}a_i = \lambda_{kj}a_j$; wegen der Verträglichkeit der λ_{ji}, d.h. der Kommutativität des Diagramms

$$\begin{array}{ccc} A_i & \xrightarrow{\lambda_{ki}} & A_k \\ {\scriptstyle\phi_i}\downarrow & & \downarrow{\scriptstyle\phi_k} \\ B_i & \xrightarrow{\mu_{ki}} & B_k, \end{array}$$

gilt $\phi_k(a_k) = \phi_k\lambda_{ki}(a_i) = \mu_{ki}\phi_i(a_i)$, und aus demselben Grund $\phi_k(a_k) = \mu_{kj}\phi_j(a_j)$. Also ist $\phi : A \longrightarrow B$ wohldefinierter Homomorphismus.

Sind nun alle ϕ_i injektiv und gilt $\phi(a) = 0$ für ein $a = \overline{a_i} \in A$, so folgt $\phi_i(a_i) = 0$ und damit $a_i = 0$. Also ist auch ϕ injektiv.

Sind dagegen alle ϕ_i surjektiv und ist $b = \overline{b_i} \in B$ gegeben, so wählen wir ein $a_i \in A_i$ mit $\phi_i(a_i) = b_i$; dann ist aber $\phi(\overline{a_i}) = b$.

Sind schließlich für jeden Index i exakte Sequenzen

$$0 \longrightarrow A_i \xrightarrow{\alpha_i} B_i \xrightarrow{\beta_i} C_i \longrightarrow 0$$

gegeben und die α_i und β_i mit den λ_{ji}, μ_{ji} und ν_{ji} verträglich, die zu den direkten Systemen der A_i, B_i und C_i gehören, so ist auch

$$0 \longrightarrow \varinjlim A_i \xrightarrow{\alpha} \varinjlim B_i \xrightarrow{\beta} \varinjlim C_i \longrightarrow 0$$

exakt: zu zeigen ist nur noch, daß im $\alpha = \ker \beta$ ist. Dies folgt aber mit dem bereits Bewiesenen aus $\operatorname{im} \alpha_i \simeq \ker \beta_i$ und der Tatsache, daß auch die $\operatorname{im} \alpha_i$ und $\ker \beta_i$ auf natürliche Art und Weise direkte Systeme bilden. □

Korollar 4.8. *Seien $(I, [G_i, A_i])$, $(I, [G_i, B_i])$ und $(I, [G_i, C_i])$ induktive Systeme und die Sequenz*

$$0 \longrightarrow A_i \longrightarrow B_i \longrightarrow C_i \longrightarrow 0$$

von G_i-Moduln für jedes i exakt. Dann ist auch

$$0 \longrightarrow \varinjlim A_i \longrightarrow \varinjlim B_i \longrightarrow \varinjlim C_i \longrightarrow 0$$

exakte Sequenz von G-Moduln.

Beweis. Man hat nur noch die Operation von G auf den direkten Limites zu installieren. □

Schließlich brauchen wir noch folgendes Lemma, um eine kleine Lücke in Kochs Beweis zu schließen:

Lemma 4.9. *Ist $(I, [G_i, A_i])$ ein induktives System, dann ist auch das System $(I, [G_i, M_{G_i}(A_i)])$ induktiv, und mit $G = \varprojlim G_i$ und $A = \varinjlim A_i$ gilt $M_G(A) = \varinjlim M_{G_i}(A_i)$.*

Beweis. Sei $f_i \in M_{G_i}(A_i)$; dann setzen wir $f = \lambda_i \circ f_i \circ \pi_i$, d.h. wir definieren eine Abbildung $G \longrightarrow A$ durch Komposition der kanonischen Abbildungen $G \longrightarrow G_i \longrightarrow A_i \longrightarrow A$. Mit f_i ist auch f stetig, insbesondere also Element von $M_G(A)$.

Der dadurch definierte Homomorphismus $\Psi_i : M_{G_i}(A_i) \longrightarrow M_G(A)$ induziert einen Homomorphismus $\psi : \varinjlim M_{G_i}(A_i) \longrightarrow M_G(A)$, und dieser ist injektiv: aus $f(\sigma) = 0$ mit $\sigma = (\dots, \sigma_i, \dots)$ und $\sigma_i \in G_i$ folgt $f_i(\sigma_i) \sim 0$; also gibt es einen Index $j \geq i$ mit $\lambda_{ji} f_i(\sigma_i) = 0$. Kompatibilität der λ_{ji} mit den π_{ji} zeigt, daß $f_j(\sigma_j) = 0$ ist.

Zu zeigen ist noch, daß ψ surjektiv ist. Dazu sei ein $f : G \longrightarrow A$ aus $M_G(A)$ gegeben; wir haben dann eine Abbildung $f_k : G_k \longrightarrow A_k$ zu konstruieren mit $\Psi_k(f_k) = f$. Da es nur endlich viele Bilder unter f gibt, existiert ein

Index k, sodaß im $f \subseteq \lambda_k(A_k)$ ist. Weiter gibt es einen offenen Normalteiler N derart, daß f auf den Nebenklassen von G/N konstant ist; indem wir N notfalls verkleinern, können wir annehmen, daß G_k homomorphes Bild von G/N ist. Da f über G_k faktorisiert und die Bilder in $\lambda_k(A_k)$ liegen, können wir durch $f_k(\sigma_k) = a_k$, wo $f(\sigma) = \overline{a_k}$ war, eine stetige (wegen der Endlichkeit des Bilds) Abbildung $f_k : G_k \longrightarrow A_k$ gewinnen. □

Unter den oben gemachten Voraussetzungen über das System $(I, [G_i, A_i])$ bildet auch $(\mathrm{H}^q(G_i, A_i), \mu_{ji})$ ein direktes System, wobei wir $\mu_{ji} = (\pi_{ji}, \lambda_{ji})$ gesetzt haben. Damit gilt:

Satz 4.10. *Ist $G = \varprojlim G_i$ projektiver Limes pro-endlicher Gruppen $A = \varinjlim A_i$ direkter Limes diskreter G_i-Moduln, und sind die dazugehörigen Abbildungen π_{ji} und λ_{ji} kompatibel, so wird A ein diskreter G-Modul, und es ist $\mathrm{H}^q(G, A) = \varinjlim \mathrm{H}^q(G_i, A_i)$ für jedes $q \geq 0$.*

Beweis. Wir beweisen den Satz per Dimensionsverschiebung mit Induktion. Für $q = 0$ ist zu zeigen, daß $\varinjlim A_i^{G_i} = A^G$ gilt. Ist $a_i \in A_i^{G_i}$, weiter $\sigma = (\dots \sigma_i, \dots) \in G$ und gilt $\sigma_i a_i = a_i$, dann folgt sofort $\sigma a = a$.

Die Umkehrrichtung ist etwas schwieriger, weil der naive Zugang scheitert: aus $a = \overline{a_i} \in A^G$ folgt erst einmal nur, daß $\sigma_i a_i \sim a_i$ gilt. Dies impliziert aber die Existenz eines $k \geq i$ mit $\lambda_{ki}\sigma_i a_i = \lambda_{ki} a_i$. Wegen $\sigma_i = \pi_{ki}\sigma_k$ bedeutet dies $\lambda_{ki} a_i = \lambda_{ki}\pi_{ki}\sigma_k a_i$, und aus der Kompatibilität von π mit λ folgt dann $\lambda_{ki} a_i = \sigma_k \lambda_{ki} a_i$. Dies heißt nun aber nicht, daß $a_k := \lambda_{ki} a_i$ in $A_K^{G_k}$ liegt: unser Index k hängt ja von σ_i ab. Um für alle $\sigma_i \in G_i$ einen Index k zu finden, der es tut, muß man die Tatsache benutzen, daß die A_i diskrete G_i-Moduln sind. In der Tat, sind beispielsweise alle G_i endlich, so ist es kein Problem, aus den endlich vielen Indizes k, die zu den σ_i gehören, einen Index j zu finden, der für alle σ_i gut ist. Der allgemeine Fall geht so: da A_i diskreter G_i-Modul ist, hat a_i nur endlich viele Bilder unter der Operation von G_i; diese endlich vielen Bilder kommen von endlich vielen σ_i, und zu diesen endlich vielen findet man wie oben einen globalen Index k mit den gewünschten Eigenschaften.

Sei die Behauptung nun für ein $q \geq 0$ bewiesen. Aus der Existenz des folgenden kommutativen Diagramms mit exakten Zeilen

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_i & \longrightarrow & M_{G_i}(A_i) & \longrightarrow & C_i & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_j & \longrightarrow & M_{G_j}(A_j) & \longrightarrow & C_j & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \longrightarrow & M_G(A) & \longrightarrow & C & \longrightarrow & 0.
\end{array}$$

erhalten wir (unter Berücksichtigung von Lemma 4.9 und der Tatsache, daß der direkte Limes ein exakter Funktor in der Kategorie der abelschen Gruppen

ist, das exakte kommutative Diagramm

$$\begin{array}{ccccccc}
\varinjlim \mathrm{H}^q(G_i, M_{G_i}(A_i)) & \longrightarrow & \varinjlim \mathrm{H}^q(G_i, C_i) & \longrightarrow & \varinjlim \mathrm{H}^{q+1}(G_i, A_i)) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathrm{H}^q(G, M_G(A)) & \longrightarrow & \mathrm{H}^q(G, C) & \longrightarrow & \mathrm{H}^{q+1}(G, A) & \longrightarrow & 0,
\end{array}$$

Nach Induktionsvoraussetzung sind die Abbildungen in den beiden linken Spalten Isomorphismen; fügt man an das Diagramm rechts noch eine Spalte Nullen an, so folgt aus dem Fünferlemma, daß auch $\varinjlim \mathrm{H}^{q+1}(G_i, A_i)) \longrightarrow \mathrm{H}^{q+1}(G, A)$ ein Isomorphismus ist (für $q \geq 1$ ist das Argument noch einfacher, weil die linke Spalte dann verschwindet). □

Literatur

Eine Kohomologie von Gruppen mit Betonung auf Gruppentheorie wird in Brown [2] präsentiert. Die Klassenkörpertheorie von Artin und Tate [1] enthält ein ganzes Kapitel (das vorvorletzte) über die Theorie der Gruppenerweiterungen (die im wesentlichen Ende der 20er Jahre von Schreier entworfen wurde). In der Tat kenne ich keine vergleichbare Diskussion solcher Objekte, in denen z.B. auch auf die Frage eingegangen wird, wie sich kohomologische Abildungen wie die Inflation konkret in der Theorie der Gruppenerweiterungen widerspiegeln.

Eine Einführung in die Theorie der Brauergruppen findet man in Farb & Dennis [3], eine Monographie über die Dinger hat Ina Kersten [5] geschrieben. Ebenfalls zu erwähnen sind hier die Algebrabände von Jacobson [4].

1. E. Artin, J. Tate, *Class Field Theory*, Addison-Wesley 1967, 1990

2. K.S. Brown, *Cohomology of groups*, Springer GTM 87, 1982, 1994

3. B. Farb, R.K. Dennis, *Noncommutative algebra*, GTM 144, Springer-Verlag 1993

4. N. Jacobson, *Basic Algebra I, II*, New York, 1989

5. I. Kersten, *Brauergruppen von Körpern*, Vieweg 1990