Galoismoduln mit Hasse-Prinzip

Von *Uwe Jannsen* in Regensburg

O. Neumann [6] stellte die Frage, ob jeder irreduzible endliche Galoismodul ein Modul mit Hasse-Prinzip ist. Dies läßt sich positiv beantworten, wenn die trivialisierende Erweiterung eine auflösbare Galoisgruppe besitzt. Im Gegensatz hierzu gibt es bereits für die kleinste nicht-auflösbare Gruppe A_5 Moduln, die dem Hasse-Prinzip nicht genügen.

Sei k ein endlich-algebraischer Zahlkörper mit separablem Abschluß $\bar{k}$ und $G_k = \mathrm{Gal}(\bar{k}/k)$ die absolute Galoisgruppe. Ein endlicher G_k-Modul A heißt nach Neumann Modul mit Hasse-Prinzip, wenn die Lokalisierungsabbildung

$$\alpha(k, A)\colon H^1(k, A) \to \prod_{\mathfrak{p}} H^1(k_{\mathfrak{p}}, A)$$

injektiv ist; hierbei durchläuft $\mathfrak{p}$ alle Primstellen von k, und $k_{\mathfrak{p}}$ ist die Lokalisierung von k bezüglich $\mathfrak{p}$. Zur Bedeutung dieser Frage, insbesondere für Einbettungsprobleme, vergleiche man [5] und [6].

Für reduzible Moduln A ist i.a. $\mathrm{Ker}\,\alpha(k, A) \neq 0$, siehe [6] § 3 und [4] 7.3. Bezeichnet $k(A)$ die trivialisierende Erweiterung von A, die galoistheoretisch zum Kern der Abbildung $G_k \to \mathrm{Aut}(A)$ gehört, so soll dagegen gezeigt werden:

Satz 1. *Sei A ein endlicher, einfacher G_k-Modul, $pA = 0$ für die Primzahl p und die Galoisgruppe von $k(A)/k$ p-auflösbar. Dann ist*

i) *die Abbildung*

$$\beta(k, A)\colon H^2(k, A) \to \prod_{\mathfrak{p}} H^2(k_{\mathfrak{p}}, A)$$

injektiv,

ii) *für jede Primstellenmenge S von k mit Dirichletdichte $\delta(S) = 1$ die Abbildung*

$$\alpha(k, S, A)\colon H^1(k, A) \to \prod_{\mathfrak{p} \in S} H^1(k_{\mathfrak{p}}, A)$$

injektiv.

0075-4102/82/0337-0009$02.00

Zum Beweis benötigen wir einige Vorbetrachtungen.

Definition (vergl. [7] § 2). Für eine pro-endliche Gruppe G und einen diskreten G-Modul A sei $H^1_*(G, A)$ der Kern der von den Restriktionen induzierten Abbildung

$$\varphi(G, A)\colon H^1(G, A) \to \prod_Z H^1(Z, A),$$

wobei Z alle (im pro-endlichen Sinne) zyklischen Untergruppen von G durchläuft. Insbesondere sei $H^1_*(k, A) = H^1_*(G_k, A)$ für einen G_k-Modul A gesetzt.

Lemma 1. *Sei A ein endlicher G_k-Modul, S eine Menge von Primstellen von k mit $\delta(S)=1$ und $K \supseteqq k(A)$ eine Erweiterung, die galoissch über k ist. Ist $S(K)$ die Menge der über S liegenden Primstellen von K, $G_{\mathfrak{P}}$ die Zerlegungsgruppe von $\mathfrak{P} \in S(K)$ in $G = \mathrm{Gal}(K/k)$ und*

$$\alpha(K/k, S, A)\colon H^1(G, A) \to \prod_{\mathfrak{P} \in S(K)} H^1(G_{\mathfrak{P}}, A)$$

die von den Restriktionen induzierte Abbildung, so gelten die Beziehungen

$$\begin{array}{ccc}
\operatorname{Ker} \alpha(K/k, S, A) & \xrightarrow[\sim]{\mathrm{Inf}} & \operatorname{Ker} \alpha(k, S, A) \\
\cap\!\shortparallel & & \cap\!\shortparallel \\
H^1_*(G, A) & \xrightarrow[\sim]{\mathrm{Inf}} & H^1_*(k, A)
\end{array} .$$

Die Inklusionen werden zu Gleichheiten, wenn alle $G_{\mathfrak{P}}$ zyklisch sind.

Beweis. Aus der Hochschild-Serre-Sequenz erhält man das exakte kommutative Diagramm

$$\begin{tikzcd}
0 \arrow[r] & \prod\limits_{\mathfrak{P} \in S(K)} H^1(G_{\mathfrak{P}}, A) \arrow[r] & \prod\limits_{\mathfrak{P} \in S(K),\, \mathfrak{P}/\mathfrak{p}} H^1(k_{\mathfrak{p}}, A) \arrow[r] & \prod\limits_{\mathfrak{P} \in S(K)} H^1(K_{\mathfrak{P}}, A) \\
0 \arrow[r] & H^1(G, A) \arrow[u, "\alpha(K/k, S, A)"'] \arrow[r, "\mathrm{Inf}"] & H^1(k, A) \arrow[u] \arrow[r] & H^1(K, A), \arrow[u, "\alpha(K, S(K), A)"']
\end{tikzcd}$$

in dem $\alpha(K, S(K), A)$ nach dem Tschebotoreff'schen Dichtigkeitssatz injektiv ist, da G_K trivial auf A operiert. Die Inflation vermittelt daher einen Isomorphismus von $\operatorname{Ker} \alpha(K/k, S, A)$ auf den Kern der mittleren Abbildung, der offenbar gleich $\operatorname{Ker} \alpha(k, S, A)$ ist. Die Inklusion $\operatorname{Ker} \alpha(K/k, S, A) \subseteqq H^1_*(G, A)$ gilt, da wiederum nach dem Tschebotoreff'schen Dichtigkeitssatz alle zyklischen Untergruppen von G unter den $G_{\mathfrak{P}}$ vorkommen. Die Isomorphie $H^1_*(G, A) \rightleftarrows H^1_*(k, A)$ folgt wieder aus der Hochschild-Serre-Sequenz, alles weitere ist dann klar.

Bemerkung. Ist G eine endliche Gruppe, so gibt es eine galoissche, unverzweigte Erweiterung K/k algebraischer Zahlkörper mit $\mathrm{Gal}(K/k) \cong G$, siehe [3]. Insbesondere sind dann alle Zerlegungsgruppen zyklisch, und für jeden endlichen G-Modul A (der durch die Projektion $G_k \twoheadrightarrow G$ zum G_k-Modul wird) ist

$$\mathrm{Ker}\,\alpha(k, A) = H^1_*(G, A).$$

Will man also eine allgemeine, vom Körper k unabhängige Lösung der von O. Neumann gestellten Frage, so muß man untersuchen, für welche Gruppen G gilt, daß $H^1_*(G, A) = 0$ für alle einfachen G-Moduln A ist.

Definition. Eine endliche Gruppe G heißt Gruppe mit Hasse-Prinzip (für die Primzahl p), wenn $H^1_*(G, A) = 0$ für alle einfachen, endlichen G-Moduln A (mit $pA = 0$) ist.

Lemma 2. *Ist* $1 \to H \to E \to G \to 1$ *eine exakte Sequenz von endlichen Gruppen, so gilt:*

i) *Sind H und G Gruppen mit Hasse-Prinzip für p, so auch E.*

ii) *Ist E Gruppe mit Hasse-Prinzip für p, so auch G.*

Beweis. i) Für einen einfachen $\mathbb{F}_p[E]$-Modul A ist entweder $A^H = 0$ oder $A^H = A$. Im ersten Fall zeigt die Hochschild-Serre-Sequenz, daß im kommutativen Diagramm

$$(1)\qquad \begin{tikzcd} \prod\limits_Z H^1(Z, A) \arrow[r, "\prod \mathrm{Res}"] & \prod\limits_Z H^1(Z \cap H, A) \\ H^1(E, A) \arrow[u, "\varphi(E, A)"] \arrow[r, hook, "\mathrm{Res}"] & H^1(H, A) \arrow[u] \end{tikzcd}$$

die untere Restriktion injektiv ist. Ist nun H eine Gruppe mit Hasse-Prinzip für p, so ist die rechte Abbildung (und damit auch $\varphi(E, A)$) injektiv, denn $Z \cap H$ durchläuft alle zyklischen Untergruppen von H, und nach dem Satz von Clifford (s. [2] 2. 2) ist A direkte Summe einfacher $\mathbb{F}_p[H]$-Moduln.

Für $A^H = A$ erhält man das exakte kommutative Diagramm

$$(2)\qquad \begin{tikzcd} 0 \arrow[r] & \prod\limits_Z H^1(ZH/H, A) \arrow[r] & \prod\limits_Z H^1(Z, A) \arrow[r] & \prod\limits_Z H^1(Z \cap H, A) \\ 0 \arrow[r] & H^1(G, A) \arrow[u] \arrow[r] & H^1(E, A) \arrow[u, "\varphi(E, A)"'] \arrow[r] & H^1(H, A). \arrow[u] \end{tikzcd}$$

Die rechte vertikale Abbildung ist injektiv, da A ein trivialer H-Modul ist und die $Z \cap H$ ganz H erzeugen, während der Kern der linken Abbildung gleich $H^1_*(G, A)$ ist, da die ZH/H alle zyklischen Untergruppen von $G = E/H$ durchlaufen.

ii) folgt sofort aus dem Diagramm (2), da jeder einfache G-Modul A auch ein einfacher E-Modul mit $A^H = A$ ist.

Corollar 1. a) *Eine endliche Gruppe G ist eine Gruppe mit Hasse-Prinzip für p, wenn dies für alle Kompositionsfaktoren von G gilt.*

b) *Eine p-auflösbare Gruppe ist eine Gruppe mit Hasse-Prinzip für p.*

c) *Eine auflösbare Gruppe ist eine Gruppe mit Hasse-Prinzip.*

Beweis. a) folgt aus Lemma 2i) durch Induktion, b) folgt aus a), da für zyklische Gruppen und Gruppen, deren Ordnung prim zu p ist, sogar $H^1_*(G, A) = 0$ für alle $\mathbb{F}_p[G]$-Moduln A ist.

Beweis von Satz 1. ii) folgt mit Lemma 1 aus Corollar 1b).

Nach dem Dualitätssatz von Tate und Poitou sind die Kerne von $\beta(k, A)$ und $\alpha(k, A')$ isomorph, wobei $A' = \mathrm{Hom}(A, \bar{k}^*)$ der zu A duale G_k-Modul ist. Weiter ist mit A auch A' einfach und mit $k(A)/k$ auch die Erweiterung $k(A')/k$ auflösbar, als Teilerweiterung der auflösbaren Erweiterung $k(A)(\mu_p)/k$, μ_p die Gruppe der p-ten Einheitswurzeln in $\bar{k}$. Daher folgt i) aus ii).

Bemerkungen. 1) Ein anderer Beweis für Corollar 1b) ergibt sich daraus, daß für eine p-auflösbare Gruppe G gerade $H^1\big(G/C(A), A\big) = 0$ für alle einfachen $\mathbb{F}_p[G]$-Moduln A gilt, wobei $C(A) = \mathrm{Ker}\big(G \to \mathrm{Aut}(A)\big)$ der Zentralisator von A in G ist, s. [9].

2) Für einfache $\mathbb{F}_p[G]$-Moduln A, die nicht im prinzipalen Block von $\mathbb{F}_p[G]$ liegen, ist $H^i(G, A) = 0$ für alle $i \geqq 0$, also insbesondere $H^1_*(G, A) = 0$.

3) Es sei an dieser Stelle erwähnt, daß der Beweis von 1. 3b) in [6] eine Lücke enthält, da er die Ungleichung $k(A) \neq k(A) \cap k(A')$ benutzt, die äquivalent zu $k(A) \nsubseteq k(A')$ $\big($bzw. $\mu_p \nsubseteq k(A')\big)$ ist und nicht aus $k(A) \neq k(A')$ folgt.

Nicht-auflösbare Gruppen. Die kleinste nicht-auflösbare Gruppe $G = A_5$ (die alternierende Gruppe vom Grad 5) besitzt 4 irreduzible $\bar{\mathbb{F}}_2[G]$-Moduln, siehe [8] 18. 6. Für die Moduln A der Dimension 1 und 4 ist $H^1(G, A) = 0$ $\big($der vierdimensionale Modul ist die spezielle Darstellung von G und daher projektiv, vergl. [8] 16. 4. Prop. 4b)$\big)$. Die beiden übrigen Moduln leiten sich aus dem Isomorphismus $A_5 \cong SL_2(\mathbb{F}_4)$ und der natürlichen, 2-dimensionalen $\mathbb{F}_4$-Darstellung V von $SL_2(\mathbb{F}_4)$ ab. Es ist $H^1(Z, V) = 0$ für die zyklischen 2-Untergruppen Z von $SL_2(\mathbb{F}_4)$ $\Big($für $Z = \Big\langle \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \Big\rangle$ ist $\hat{H}^0(Z, V) = 0$, alle zyklischen 2-Untergruppen sind zu einer von dieser Form konjugiert$\Big)$. Wäre nun $\varphi(G, A)$ injektiv für alle einfachen $\bar{\mathbb{F}}_2[G]$-Moduln, so wäre $H^1(G, V) = 0$ und damit $H^1(G, A) = 0$ für alle einfachen $\mathbb{F}_2[G]$-Moduln, also für alle $\bar{\mathbb{F}}_2[G]$-Moduln, was nicht sein kann.

Dies Beispiel ist nicht singulär. In der Tat kann man mit den Methoden aus [1] § 6 ausrechnen, daß für die natürliche, irreduzible Darstellung von $SL_2(\mathbb{F}_{2^r})$ auf $V = \mathbb{F}_{2^r} \times \mathbb{F}_{2^r}$ immer $H^1\big(SL_2(\mathbb{F}_{2^r}), V\big) \cong \mathbb{F}_{2^r}$ gilt $\big($vergl. auch [1] Tab. (4. 5)$\big)$, während $H^1(Z, V) = 0$ für alle zyklischen 2-Untergruppen Z ist.

Obwohl A_5 nicht 3- oder 5-auflösbar ist, ist A_5 eine Gruppe mit Hasse-Prinzip für $p = 3$ und $p = 5$, da die 3- und 5-Sylowgruppen zyklisch sind. Ist aber vielleicht eine Gruppe genau dann auflösbar, wenn sie das Hasse-Prinzip für 2 erfüllt? Man beachte, daß eine Gruppe mit zyklischen 2-Sylowgruppen auflösbar ist und daß nach dem Satz von Feit und Thompson 2-auflösbar gleich auflösbar ist.

Literatur

[1] *E. Cline, B. Parshall, L. Scott*, Cohomology of finite groups of Lie type. I, Publ. Math. I.H.E.S. **45** (1975), 169—191.
[2] *J. D. Dixon, B. M. Puttaswamaiah*, Modular Representations of Finite Groups, New York-London 1977.
[3] *A. Fröhlich*, On non-ramified extensions with prescribed Galois group, Mathematica **9** (1962), 133—134.
[4] *K. Haberland*, Galois Cohomology of Algebraic Number Fields, Berlin 1978.
[5] *J. Neukirch*, Über das Einbettungsproblem der algebraischen Zahlentheorie, Inv. math. **21** (1973), 59—116.
[6] *O. Neumann*, Einige Klassen von endlichen Galois-Moduln mit Hasse-Prinzip, Math. Nachr. **72** (1976), 305—320.
[7] *J.-P. Serre*, Sur les groupes de congruence des variétés abéliennes, Izv. Akad. Nauk. SSSR **28** (1964), 3—20.
[8] *J.-P. Serre*, Linear Representations of Finite Groups, GTM **42**, Berlin-Heidelberg-New York 1977.
[9] *U. Stammbach*, Cohomological characterisations of finite solvable and nilpotent groups, J. Pure and Appl. Alg. **11** (1977), 293—301.

Universität Regensburg, Fakultät für Mathematik, Universitätsstraße 31, D-8400 Regensburg

Eingegangen 11. März 1982