WIKIPEDIA

Frobeniushomomorphismus

Der **Frobeniushomomorphismus** ist in der Algebra ein Endomorphismus von Ringen, deren Charakteristik eine Primzahl ist. Der Frobeniushomomorphismus ist nach dem deutschen Mathematiker Ferdinand Georg Frobenius benannt.

Inhaltsverzeichnis

Frobeniusendomorphismus eines Rings

Definition

Es sei R ein kommutativer unitärer Ring mit der Charakteristik p, wobei p eine Primzahl ist. Als Frobeniushomomorphismus wird die Abbildung

$$\phi_p\colon R \to R,\ \ x \mapsto x^p$$

bezeichnet. Sie ist ein Ringhomomorphismus.

Ist $q = p^e$, dann ist auch

$$\phi_q = \phi_p^e\colon R \to R,\ \ x \mapsto x^q$$

ein Ringhomomorphismus.

Beweis der Homomorphieeigenschaft

Die Abbildung ϕ_p ist verträglich mit der Multiplikation in R, da aufgrund der Potenzgesetze

$$\phi_p(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = \phi_p(x) \cdot \phi_p(y)$$

gilt. Ebenso gilt $\phi_p(1) = 1^p = 1$. Interessanterweise ist die Abbildung zudem mit der Addition in R verträglich, das heißt, es gilt $\phi_p(x+y) = \phi_p(x) + \phi_p(y)$. Mit Hilfe des Binomialsatzes folgt nämlich

$$(x+y)^p = x^p + \left(\sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k \right) + y^p$$

Da p eine Primzahl ist, teilt p zwar $p!$ aber nicht $m!$ für $m < p$. Da die Charakteristik p deshalb den Zähler, aber nicht den Nenner der Binomialkoeffizienten

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

teilt, verschwinden die Binomialkoefizienten in der obigen Formel. Die Addition vereinfacht sich zu

$$(x+y)^p = x^p + y^p$$

und ist verträglich mit der Addition in R. Diese Gleichung wird im englischsprachigen Raum als *Freshman's Dream* (der Traum des Anfängers) bezeichnet.

Verwendung

Im Folgenden ist p stets eine Primzahl und q eine Potenz von p. Alle vorkommenden Ringe oder Körper haben Charakteristik p.

- Nach dem Kleinen Satz von Fermat ist ϕ_p auf dem Restklassenring $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ die Identität. Allgemeiner: Ist $\mathbb{F}_q$ ein endlicher Körper, dann ist ϕ_q die Identität.
- Ist K ein Körper, dann ist $\{x \in K : \phi_p(x) = x\} = \mathbb{F}_p$.
- Ist $\mathbb{F}_{q^n}/\mathbb{F}_q$ eine Erweiterung endlicher Körper, dann ist ϕ_q ein Automorphismus von $\mathbb{F}_{q^n}$, der $\mathbb{F}_q$ elementweise fest lässt. Die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ ist zyklisch und wird von ϕ_q erzeugt.
- Ist A ein Ring, dann ist $\phi_p \colon A \to A$ genau dann injektiv, wenn A keine nichttrivialen nilpotenten Elemente enthält. (Der Kern von ϕ_p ist $\{a \in A : a^p = 0\}$.)
- Ist A ein Ring und ist $\phi_p \colon A \to A$ bijektiv, dann heißt der Ring perfekt (oder vollkommen).[1] In einem perfekten Ring besitzt jedes Element eine eindeutig bestimmte p-te Wurzel. Perfekte Körper zeichnen sich dadurch aus, dass sie keine inseparablen Erweiterungen besitzen.
- Der perfekte Abschluss eines Rings A lässt sich als induktiver Limes darstellen:

$$A^{p^{-\infty}} = \varinjlim \left(A \xrightarrow{\phi_p} A \xrightarrow{\phi_p} A \xrightarrow{\phi_p} \dots \right)$$

- Die Additivität der Abbildung $x \mapsto x^p$ wird auch in der Artin-Schreier-Theorie ausgenutzt.

Frobeniusautomorphismen von lokalen und globalen Körpern

Die folgenden Annahmen dienen dazu, sowohl den Fall einer endlichen Galoiserweiterung algebraischer Zahlkörper als auch lokaler Körper zu beschreiben. Sei A ein Dedekindring, K sein Quotientenkörper, L/K eine endliche Galoiserweiterung, B der ganze Abschluss von A in L. Dann ist B ein Dedekindring. Sei weiter $\mathfrak{P}$ ein maximales Ideal in B mit endlichem Restklassenkörper $\lambda = B/\mathfrak{P}$, außerdem $\mathfrak{p} = \mathfrak{P} \cap A$ und $\kappa = A/\mathfrak{p}$. Die Körpererweiterung λ/κ ist galoissch. Sei G die Galoisgruppe von L/K. Sie operiert transitiv auf den über $\mathfrak{p}$ liegenden Primidealen von B. Sei $G_{\mathfrak{P}}$ die Zerlegungsgruppe, d. h. der Stabilisator von $\mathfrak{P}$. Der induzierte Homomorphismus

$$r : G_{\mathfrak{P}} \to \mathrm{Gal}(\lambda/\kappa)$$

ist surjektiv.[2] Sein Kern ist die Trägheitsgruppe.

Es sei nun $\mathfrak{P}$ unverzweigt, d. h. $\mathfrak{p}B_{\mathfrak{P}} = \mathfrak{P}$. Dann ist der Homomorphismus r ein Isomorphismus. Der Frobeniusautomorphismus $\mathbf{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ (auch Frobeniuselement) ist das Urbild des Frobeniusautomorphismus $\phi_{|\kappa|} \in \mathrm{Gal}(\lambda/\kappa)$ unter r. Er ist durch die folgende Eigenschaft eindeutig charakterisiert:

$$\mathbf{Frob}_{\mathfrak{P}} b \equiv b^{|\kappa|} \mod \mathfrak{P}$$

Weil G auf den Primidealen über $\mathfrak{p}$ transitiv operiert, sind die Frobeniusautomorphismen zu ihnen konjugiert, so dass ihre Konjugationsklasse durch $\mathfrak{p}$ eindeutig festgelegt ist. Falls die Erweiterung L/K abelsch ist, erhält man einen eindeutigen Frobeniusautomorphismus $\mathbf{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$.

Frobeniusautomorphismen sind von zentraler Bedeutung für die Klassenkörpertheorie. In der idealtheoretischen Formulierung wird die Reziprozitätsabbildung von der Zuordnung $\mathfrak{p} \mapsto \mathbf{Frob}_{\mathfrak{p}}$ induziert. Konjugationsklassen von Frobeniusautomorphismen sind der Gegenstand des tschebotarjowschen Dichtigkeitssatzes. Ferdinand Georg Frobenius hatte die Aussage des Dichtigkeitssatzes bereits 1880 vermutet, deshalb sind die Automorphismen nach ihm benannt.[3]

Absoluter und relativer Frobenius für Schemata

Definition

Sei p eine Primzahl und X ein Schema über $\mathbb{F}_p$. Der absolute Frobenius $\phi_X\colon X \to X$ ist definiert als Identität auf dem topologischen Raum und p-Potenzierung auf der Strukturgarbe. Auf einem affinen Schema $\mathbf{Spec}\ A$ ist der absolute Frobenius durch den Frobenius des zugrundeliegenden Ringes gegeben, wie man an den globalen Schnitten ablesen kann. Dass die Primideale fest bleiben, übersetzt sich in die Äquivalenz $a \in \mathfrak{p} \iff a^p \in \mathfrak{p}$.

Sei nun $X \to S$ ein Morphismus von Schemata über $\mathbb{F}_p$. Das Diagramm

$$\begin{array}{ccc} X & \xrightarrow{\phi_X} & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{\phi_S} & S \end{array}$$

kommutiert und induziert den relativen Frobeniusmorphismus

$$F_{X/S}\colon X \to X^{(p/S)} = S \times_{\phi_S, S} X$$

der ein Morphismus über S ist. Ist $S = \mathbf{Spec}\ A$ das Spektrum eines perfekten Rings A, dann ist ϕ_S ein Isomorphismus, also $X^{(p/S)} \cong X$, aber dieser Isomorphismus ist im Allgemeinen kein Morphismus über S.

Beispiel

- Mit $X = S[T_1, \ldots, T_n]$ ist $X^{(p)} \cong S[T_1, \ldots, T_n]$ (über S), und der relative Frobenius ist in Koordinaten gegeben durch:

  $$T_i \mapsto T_i^p$$

- Ist $B = A[T_1, \ldots, T_n]/(f_1, \ldots, f_m)$, dann ist $(\mathbf{Spec}\ B)^{(p/\mathrm{Spec}\ A)} = A[T_1^p, \ldots, T_n^p]/(\tilde{f}_1, \ldots, \tilde{f}_m)$, wobei $\tilde{f}$ bedeuten soll, dass die Koefizienten in die p-te Potenz erhoben werden. Der relative Frobenius $(\mathbf{Spec}\ B)^{(p/\mathrm{Spec}\ A)} \to B$ wird von $T_i \mapsto T_i^p$ induziert.

Eigenschaften

- $F_{X/S}$ ist ganz, surjektiv und radiziell. Für X/S lokal von endlicher Präsentation ist $F_{X/S}$ genau dann ein Isomorphismus, wenn X/S étale ist.[4]
- Wenn X/S flach ist, besitzt $X^{(p/S)}$ die folgende lokale Beschreibung: Sei $\mathbf{Spec}\ A$ eine offene affine Karte von X. Mit der symmetrischen Gruppe S_p und $N = \sum_{\sigma \in S_p} \sigma$ setze $A^{(p)} = (A^{\otimes p})^{S_p} / N \cdot A^{\otimes p}$. Die Multiplikation definiert einen Ringhomomorphismus $A^{(p)} \to A$, und durch Verkleben von $\mathbf{Spec}\ A^{(p)}$ erhält man das Schema $X^{(p)}$.[5]

Satz von Lang

Ein Satz von Serge Lang besagt: Sei G ein algebraisches oder affines zusammenhängendes Gruppenschema über einem endlichen Körper $\mathbb{F}_q$. Dann ist der Morphismus

$$L : x \mapsto x^{-1} \cdot F_q(x)$$

treuflach. Ist G algebraisch und kommutativ, ist L also eine Isogenie mit Kern $G(\mathbb{F}_q)$, die Lang-Isogenie. Ein Korollar ist, dass jeder G-Torsor trivial ist.[6]

Beispiele:

- Für $G = \mathbb{G}_a$ erhält man den Artin-Schreier-Morphismus
- Für $G = \mathrm{GL}_n$ erhält man die Aussage, dass jede zentrale einfache Algebra vom Rang n über einem endlichen Körper eine Matrizenalgebra ist, für alle n zusammengenommen also den Satz von Wedderburn.

Frobenius und Verschiebung für kommutative Gruppen

Sei S ein Schema und G/S ein flaches kommutatives Gruppenschema. Die obige Konstruktion realisiert $G^{(p/S)}$ als Unterschema des symmetrischen Produkts G^p/S_p (falls dieses existiert, andernfalls muss man mit einem kleineren Unterschema von G^p arbeiten), und durch Verkettung mit der Gruppenmultiplikation erhält man einen kanonischen Morphismus $V_{G/S} \colon G^{(p/S)} \to G$, die Verschiebung. Der Name kommt daher, dass die Verschiebung bei Wittvektoren die Abbildung

$$(x_0, x_1, x_2, \ldots) \mapsto (0, x_0, x_1, \ldots)$$

ist.

Es gilt:[7]

- $$V_{G/S} \circ F_{G/S} = p, \quad F_{G/S} \circ V_{G/S} = p$$

  (Multiplikation mit p in der Gruppe G bzw. $G^{(p)}$).
- $\mathrm{Lie}(G/S) = \mathrm{Lie}(\ker(F_{G/S})/S)$
- Ist G/S ein endliches flaches kommutatives Gruppenschema, dann vertauscht die Cartier-Dualität Frobenius und Verschiebung:

  $$F_{D(G)/S} = D(V_{G/S}), \quad V_{D(G)/S} = D(F_{G/S})$$

Eine endliche kommutative Gruppe G über einem Körper ist genau dann

- vom multiplikativen Typ, wenn V ein Isomorphismus ist.
- étale, wenn F ein Isomorphismus ist.
- infinitesimal, wenn $F^n = 0 \colon G \to G^{(p^n)} = ((G^{(p)}) \ldots)^{(p)}$ für n groß.
- unipotent, wenn $V^n = 0 \colon G^{(p^n)} \to G$ für n groß.

Die Charakterisierung von Gruppen durch Eigenschaften von F und V ist der Ausgangspunkt der Dieudonné-Theorie.

Beispiele:

- Für konstante Gruppen ist $F = \mathrm{id}$ und $V = p$.
- Für diagonalisierbare Gruppen ist $F = p$ und $V = \mathrm{id}$.
- Für $G = \mathbb{G}_a$ ist F der gewöhnliche Frobeniushomomorphismus $\phi_p\colon A \to A$ für Ringe $A = \mathbb{G}_a(A)$. (Da der Frobeniusmorphismus ohne Rückgriff auf die Gruppenstruktur definiert ist, ist die Inklusion $\mathbb{G}_m(A) \subseteq \mathbb{G}_a(A)$ mit ihm kompatibel.) Die Verschiebung ist trivial: $V = 0$.
- Ist X eine abelsche Varietät über einem Körper der Charakteristik p (allgemeiner ein abelsches Schema), dann ist die folgende Sequenz exakt, wenn ${}_F X$ jeweils für den Kern des entsprechenden Morphismus $F\colon X \to Y$ steht:[8]

$$0 \to {}_{F^n}X \to {}_{p^n}X \xrightarrow{F^n} {}_{V^n}X^{(p^n)} \to 0$$

Arithmetischer und geometrischer Frobenius

Sei X ein Schema über $k = \mathbb{F}_q$, weiter $\bar{k}$ ein algebraischer Abschluss von k und $\overline{X} = X \times_{\mathrm{Spec}\ k} \mathrm{Spec}\ \bar{k}$. Der Frobeniusautomorphismus $\phi_q \in \mathrm{Gal}(\bar{k}/k)$ wird in diesem Kontext arithmetischer Frobenius genannt, der inverse Automorphismus ϕ_q^{-1} geometrischer Frobenius. Weil $\overline{X}$ über k definiert ist, ist $\overline{X}^{(q/\bar{k})} \cong \overline{X}$, und der relative Frobenius ist $F_{\overline{X}/\bar{k}} = \phi_{q,X} \times \mathrm{id}_{\bar{k}}$. Es gilt (auch nach der definierenden Gleichung des relativen Frobenius)

$$\phi_{q,\overline{X}} = (\mathrm{id}_X \times \phi_{q,\bar{k}}) \circ (\phi_{q,X} \times \mathrm{id}_{\bar{k}})$$

Ist G eine konstante Garbe auf $\overline{X}_{\mathrm{et}}$, induziert $\phi_{q,\overline{X}}$ die Identität auf der Kohomologie von G, so dass nach der obigen Gleichung der relative Frobenius $\phi_{q,X} \times \mathrm{id}_{\bar{k}}$ mit seiner aus der Geometrie kommenden Komponente $\phi_{q,X}$ und der geometrische Frobenius $\mathrm{id}_X \times \phi_{q,\bar{k}}^{-1}$ dieselbe Wirkung haben.[9]

Literatur

- Serge Lang: *Algebra* (= *Graduate Texts in Mathematics*. Band 211). 3. Auflage. Springer, New York 2002, ISBN 0-387-95385-X.
- Michel Demazure, Pierre Gabriel: *Groupes algébriques. Tome 1*. North-Holland, Amsterdam 1970, ISBN 978-0-7204-2034-0.
- Pierre Gabriel: *Exposé VII$_A$. Étude infinitesimale des schémas en groupes.* In: Michel Demazure, Alexander Grothendieck (Hrsg.): *Séminaire de Géométrie Algébrique du Bois-Marie 1962-1964 (SGA 3): Schémas en groupes. Tome 1: Propriétés générales des schémas en groupes*. Springer, Berlin 1970, ISBN 978-3-540-05180-0
- Christian Houzel: *Exposé XV. Morphisme de Frobenius et rationalité des fonctions L.* In: Luc Illusie (Hrsg.): *Séminaire de Géometrie Algébrique du Bois-Marie 1965-66 (SGA 5): Cohomologie l-adique et Fonctions L* (= *Lecture Notes in Mathematics*). Band 589. Springer, Berlin 1977, ISBN 3-540-08248-4

Fußnoten

1. V §1 Definition 2 in: Nicolas Bourbaki: *Elements of Mathematics. Algebra II. Chapters 4-7.* Springer, Berlin 2003, ISBN 978-3-540-00706-7.
2. Lang, VII §2
3. Peter Stevenhagen, Hendrik Lenstra: *Chebotarëv and his density theorem.* In: *Mathematical Intelligencer.* Band 18, Nr. 2, 1996, S. 26–37. Die Originalarbeit ist: Georg Ferdinand Frobenius: *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe.* In: *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* 1896, S. 689–703.
4. Houzel, §1 Proposition 2
5. Gabriel, 4.2
6. Demazure-Gabriel, III §5, 7.2. Die Originalarbeit ist: Serge Lang: *Algebraic Groups Over Finite Fields.* In: *Amer. J. Math.* Band 78, Nr. 3, 1956, S. 555–563.
7. Demazure-Gabriel, II §7
8. Proposition 2.3 in: Tadao Oda: *The first de Rham cohomology group and Dieudonné modules.* In: *Annales scientifiques de l'École Normale Supérieure, Sér. 4.* Band 2, Nr. 1, 1969, S. 63–135 (online (http://www.numdam.org/i

tem?id=ASENS_1969_4_2_1_63_0).
9. Houzel, §2 Proposition 2