Serre, Jean-Pierre
Abelian ℓ-adic representations and elliptic curves. Written with the collaboration of Willem Kuyk and John Labute. (English) Zbl 0186.25701
McGill University Lecture Notes. New York-Amsterdam: W. A. Benjamin, Inc., 208 p. (1968).

Die Darlegung des Materials ist zum Teil sehr gedrängt. Sie gewinnt an Lebendigkeit durch viele Übungsaufgaben und Beispiele, Hinweise auf offene Fragen und Skizzen von möglichen Verallgemeinerungen.

Die Kapiteleinteilung lautet: I. ℓ-adic representations; II. The groups S_m; III. Locally algebraic abelian representations; IV. ℓ-adic representations attached to elliptic curves.

Sei ℓ eine Primzahl, und sei V ein endlich-dimensionaler Vektorraum über dem Körper Q_ℓ der ℓ-adischen Zahlen. Die volle lineare Gruppe $\operatorname{Aut}(V)$ ist eine ℓ-adische Liesche Gruppe. Sei K ein Körper, K_s eine separable algebraische Hülle von K, $G = \operatorname{Gal}(K_s/K)$ in der Krullschen Topologie. Eine ℓ-adische Darstellung von G (oder auch: von K) ist per definitionem ein stetiger Homomorphismus $\rho\colon G \to \operatorname{Aut}(V)$. Wichtige Beispiele treten etwa in folgenden Situationen auf:

1) Sei A eine Abelsche Mannigfaltigkeit über K von der Dimension d; wenn $\ell \neq \operatorname{char} K$, dann sei $T_\ell(A) = \varprojlim (A_\ell)_n$, der Tate-Modul, $V_\ell = T_\ell(A) \otimes_{Z_\ell} Q_\ell$. Die Gruppe $T_\ell(A)$ ist ein freier Z_ℓ -Modul vom Range $2d$, auf dem G operiert;

2) Kohomologie-Darstellungen: Sei X eine über K definierte algebraische Mannigfaltigkeit, sei $X_s = X \times_K \operatorname{Spec} K_s$. Für $\ell \neq \operatorname{char} K$ sei

$$H^i(X_s, Z_\ell) = \varprojlim H^i\left((X_s s)_{\text{ét}}, Z/\ell^n Z\right),$$

in der étale-Kohomologie, $H^i_\ell)(X_s) = H^i(X_s, Z_\ell) \otimes_{Z_\ell} Q_\ell$. Die Gruppe $H^1_\ell(X_s)$ ist ein Vektorraum, auf dem G operiert.

Verf. legt das Schwergewicht auf ℓ-adische Darstellungen von algebraischen Zahlkörpern. Sei $\rho\colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(V)$ eine ℓ-adische Darstellung des Zahlkörpers K; sei v eine Primstelle von K. Dann heißt ρ unverzweigt an der Stelle v, wenn alle zu v gehörigen Trägheitsgruppen durch ρ auf den identischen Automorphismus abgebildet werden. Wenn v unverzweigt für ρ ist und w auf $\overline{K}$ eine Fortsetzung von v bedeutet, dann ist eindeutig ein Frobenius-Element $\rho(F_w) = F_{w,\rho}$ von w in der Darstellung ρ definiert. Mit $P_{v,\rho}(T)$ bezeichnen wir das nur von v abhängige Polynom $\det(1 - F_{w,\rho}T)$. Die ℓ-adische Darstellung ρ heißt rational (bzw. ganz), wenn es eine endliche Primstellenmenge S (in K) gibt, so daß (a) ρ unverzweigt außerhalb S ist; (b) für $v \notin S$ die Koeffizienten von $P_{v,\rho}(T)$ in Q (bzw. Z) liegen. Rationale ℓ-adische Darstellungen zu verschiedenen ℓ werden nach Taniyama durch die Frobenius-Elemente miteinander verglichen, und man kommt zum wichtigen Begriff der Verträglichkeit, bzw. der strengen Verträglichkeit, worauf hier nicht im einzelnen eingegangen wird.

In Kapitel II wird zu einem algebraischen Zahlkörper K eine projektive Familie (S_m) von über Q definierten kommutativen Gruppen konstruiert. (m ist dabei bis auf Beiträge der unendlichen Primstellen ein ganzes Ideal von K.) Mit Hilfe der Klassenkörpertheorie wird zu jedem ℓ ein Homomorphismus $\varepsilon_\ell\colon G^{\text{ab}} \to S_m(Q_\ell)$ angegeben. Dabei ist G^{ab} die Galoisgruppe der maximalen abelschen Erweiterung von K. Jede endlich-dimensionale ℓ-adische Darstellung von $S_m(Q_\ell)$: $\varphi\colon S_m(Q_\ell) \to \operatorname{Aut}(V_\ell)$ liefert eine abelsche ℓ-adische Darstellung von K in V_ℓ: $\varphi \circ \varepsilon_\ell\colon G \to \operatorname{Aut}(V_\ell)$ (d.h., $\varphi \circ \varepsilon_\ell$ ist trivial auf dem Kommutator von G). Sei V_0 ein endlich-dimensionaler Vektorraum über Q. Die Vektorräume $V_\ell = V_0 \otimes Q_\ell$ liefern dann ein streng verträgliches System von rationalen abelschen halbeinfachen Darstellungen $\varepsilon_\ell\colon G^{\text{ab}} \to \operatorname{Aut}(V_\ell)$ (11.2.5. Theorem).

In Kapitel III werden sogenannte lokal algebraische abelsche ℓ-adische Darstellungen definiert. Sei zunächst K eine endliche Erweiterung von Q_p (p Primzahl), und sei $T = R_{K/Q_p}(G_{m/K})$ (R_{K/Q_p} = A. Weilscher Funktor „Erniedrigung des Definitionskörpers") der entsprechende algebraische Torus über Q. Sei V ein endlich-dimensionaler Q_p-Vektorraum und sei GL_V die zugehörige lineare Gruppe. Es ist $\mathrm{GL}_V(Q_p) = \operatorname{Aut}(V)$. Sei $\rho\colon \operatorname{Gal}(\overline{K}/K)^{\text{ab}} \to \operatorname{Aut}(V)$ eine abelsche p-adische Darstellung von K in V. Wenn $i\colon K^* \to \operatorname{Gal}(\overline{K}/K)^{\text{ab}}$ der kanonische Homomorphismus der lokalen Klassenkörpertheorie ist, dann ist $\rho \circ i\colon K^* =$

$T(Q_p) \to \operatorname{Aut}(V)$. Die Darstellung ρ heißt lokal algebraisch, wenn es einen algebraischen Morphismus $r\colon T \to \mathrm{GL}_V$ gibt, so daß $\rho \circ i(x) = r(x^{-1})$ für alle $x \in K^*$, die genügend nahe an 1 liegen. Es zeigt sich, daß dann die Einschränkung von ρ auf die Trägheitsgruppe von $\operatorname{Gal}(\overline{K}/K)^{\mathrm{ab}}$ halbeinfach ist (III. 1.1. Proposition 1).

Sei nun K ein algebraischer Zahlkörper. Die globale Darstellung ρ heißt lokal algebraisch, wenn alle lokalen Darstellungen ρ_v, (v durchläuft die Teiler von ℓ) lokal algebraisch sind. Das Hauptergebnis lautet:

Wenn ρ eine rationale lokal algebraische abelsche ℓ-adische Darstellung des Zahlkörpers K ist, dann entsteht ρ auf die oben beschriebene Weise durch eine ℓ-adische Darstellung einer passenden Gruppe S_m III. 2.3. Theorem 2).

In Kapitel IV beschäftigt sich Verf. mit elliptischen Kurven E, die über einem Zahlkörper K definiert sind. Zu jeder Primzahl ℓ gehört eine ℓ-adische Darstellung von K: $\rho_\ell\colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(V_\ell(E))$.

Übrigens wird hier zum ersten Male ein Beweis eines wichtigen Endlichkeitssatzes von I. R. Shafarevich [Proc. Int. Congr. Math. 1962, 163–176 (1963; Zbl 0126.06902)] aus der globalen Arithmetik der elliptischen Kurven dargestellt (IV,1.4).

Aus diesem Endlichkeitssatz ergeben sich folgende Tatsachen: 1) Es gibt nur endlich viele elliptische Kurven, die zu E K-isogen sind; 2) Wenn E keine komplexe Multiplikation über K hat, dann ist $V_\ell(E)$ irreduzibel für alle Primzahlen ℓ, und der endliche Galois-Modul E_ℓ ist einfach für fast alle ℓ (IV,1.4. Corollary; 2.1. Theorem).

Sei $G_\ell = \operatorname{Im}(\rho_\ell)$. Als sein Hauptergebnis betrachtet Verf. die Bestimmung der Lieschen Algebra $\mathfrak{g}_\ell \subseteq \operatorname{End} V_\ell(E)$ der ℓ-adischen Lieschen Gruppe G_ℓ. Wenn E keine komplexe Multiplikation besitzt, dann ist $\mathfrak{g}_\ell = \operatorname{End} V_\ell(E)$, d. h., G_ℓ ist offen in $\operatorname{Aut}(T_\ell(E))$ (IV, 2.2. Theorem).

Der Beweis stützt sich wesentlich auf Kapitel II und III. Damit ist eine vom Verf. aufgeworfene Frage [Izv. Akad. Nauk SSSR, Ser. Mat. 28, 3–18 (1964; Zbl 0128.15601) und Colloq. Int. Centre Nat. Rech. Sci. 143, 239–256 (1966; Zbl 0148.41502)] abschließend beantwortet.

Es wird folgender Isogeniesatz abgeleitet: Seien E, E' elliptische Kurven über K, sei ℓ eine Primzahl, und seien $V_\ell(E)$ und $V_\ell(E')$ die entsprechenden ℓ-adischen Darstellungsräume von K. Es werde vorausgesetzt, daß die Galois-Moduln $V_\ell(E)$ und $V_\ell(E')$ isomorph sind und die absolute Invariante j von E kein ganzes Element von K ist. Dann sind E und E' K-isogene Kurven (IV, 2.3. Theorem).

Verf. merkt an, daß dieser Satz wahrscheinlich ohne die Voraussetzung „j ist nicht-ganz" richtig ist.

Für den globalen Fall wird noch erörtert, wie sich G_ℓ und $\tilde{G}_\ell$ [= Bild von G_ℓ in $\operatorname{Aut}(E) = \operatorname{Aut}(T_\ell/\ell T_\ell)$] mit ℓ ändern. Nach einer unveröffentlichten Mitteilung hat Verf. inzwischen folgendes Ergebnis erzielt:

Wenn E keine komplexe Multiplikation besitzt, dann ist $G_\ell = \operatorname{Aut}(T_\ell)$ für fast alle ℓ, $\tilde{G}_\ell = \operatorname{Aut}(E_\ell)$ für fast alle ℓ.

In einem Anhang zu Kapitel IV werden ähnliche Ergebnisse für den lokalen Fall hergeleitet. Für lokale Problemstellungen vgl. auch den Anhang „Some problems on ℓ-adic cohomology" in der Arbeit von *J.-P. Serre* and *J. Tate* [Ann. Math. (2) 88, 492–517 (1968; Zbl 0172.46101)].

Reviewer: Olaf Neumann (Berlin)

For a scan of this review see the web version.

MSC:

`11-02` Research exposition (monographs, survey articles) pertaining to number theory
`14-02` Research exposition (monographs, survey articles) pertaining to algebraic geometry
`11G10` Abelian varieties of dimension > 1
`11G15` Complex multiplication and moduli of abelian varieties
`11G05` Elliptic curves over global fields

Keywords:

arithmetic algebraic geometry