Hamburger Beiträge zur Mathematik

Nr. 631, Dezember 2016

Über „lokal“ und „global“ in der Zahlentheorie

von Ernst Kleinert

Über „lokal“ und „global“ in der Zahlentheorie

1

Es ist bekannt, wie im „Jahrhundert der Topologie“[1] die Mathematik des Raums in die der Quantität eingedrungen ist. Auch die Ausdrücke „lokal“ und „global“ entstammen der Raumanschauung; dabei liegt die ursprüngliche Bedeutung von „global“, „weltweit“, nur noch da vor, wo der Begriff in einem politischen oder wirtschaftlichen Kontext gebraucht wird. Von „lokal“, „örtlich“ kann nur im Hinblick auf ein gegebenes Globales gesprochen werden; aber auch „global“, zur Metapher geworden, ist relativ: vom Sonnensystem aus gesehen ist auch unser Globus etwas recht Lokales. Das Verhältnis der beiden Begriffe ähnelt dem von „Teil“ und „Ganzem“, doch mit einer nicht leicht zu präzisierenden Nuance; das Lokale denkt man (mit Blick auf die Topologie) eher als die Elemente, aus denen das Ganze zusammengesetzt ist, die aber für sich genommen von allgemeinem Charakter sind und vom Ganzen noch nicht viel zeigen.

In der Topologie, der Mathematik von Raum und Räumen, ist das globale Objekt ein topologischer Raum, lokal sind seine Punkte zusammen mit „kleinen“ Umgebungen. Man nennt eine Eigenschaft von Räumen „lokal“, wenn ein Raum sie hat, sobald jeder seiner Punkte eine Umgebung besitzt, die sie hat. Zum Beispiel ist die Eigenschaft, eine Mannigfaltigkeit zu sein, definitionsgemäß lokal; nicht aber die Eigenschaft, kompakt oder zusammenhängend zu sein. Eine analoge Unterscheidung besteht für (reelle oder komplexe) Funktionen auf einem Raum; lokale Eigenschaften sind Stetigkeit oder Differenzierbarkeit; nicht lokal sind Eigenschaften des Funktionsverlaufs wie Beschränktheit oder Periodizität.

Betrachtet man Funktionen in der Umgebung eines festgelegten Punktes, gelangt man auf natürliche Weise zum Begriff eines lokalen Rings, dessen maximales Ideal aus den im fraglichen Punkt verschwindenden Funktionen besteht. Der algebraische Prozeß, der hier stattfindet, läßt sich von der Topologie ablösen und führt zu Lokalisierungen beliebiger (kommutativer) Ringe nach multiplikativ abgeschlossenen Teilmengen. Für die Zahlentheorie zentral sind die Lokalisierungen der Dedekindringe, deren Quotientenkörper die globalen Körper sind, nach ihren Primidealen.

2

Der Begriff des globalen Körpers wird so gut wie immer extensional eingeführt: ein globaler Körper, heißt es, ist entweder ein Zahlkörper oder der Funktionenkörper einer Kurve über einem endlichen Konstantenkörper. Dabei wird unterschlagen, daß die beiden Typen von Körpern bewertungstheoretisch charakterisiert werden können, nämlich als Körper mit einer Produktformel, bei der wenigstens eine der beteiligten Bewertungen diskret mit endlichem Restklassenkörper ist. Das bedeutet: der Körper K besitzt ein System von Absolutbeträgen $| \cdot |_v$, derart daß für jedes x fast alle Beträge $|x|_v = 1$ sind und ebenso das Produkt aller Beträge; dazu die genannte Endlichkeitsforderung.

---

1 **[D]**, S.7

Um eine erste Anschauung zu vermitteln, erinnern wir zunächst an den Approximationssatz für Bewertungen, den man so aussprechen kann: sind endlich viele paarweise unabhängige (nicht äquivalente) Bewertungen v von K gegeben, und bezeichnen wir mit (K,v) den metrischen Raum K mit der durch v definierten Metrik, so ist K bei diagonaler Einbettung dicht in dem Produkt der Räume (K,v); es ist klar, wie das in eine Eigenschaft simultaner Approximierbarkeit von Elementen von K zu übersetzen ist. Daraus folgt sofort, daß eine Produktformel nur für *unendliche* Systeme von Bewertungen bestehen kann; daß man, wenn eine solche besteht, nicht endlich viele hinzufügen oder auslassen kann, und daß die Beträge in ihren Äquivalenzklassen „richtig" gewählt sein müssen; eine solche Formel ist also etwas ziemlich Rigides. Weiter ist leicht zu sehen, daß höchstens endliche viele Beträge archimedisch sein können; denn weil es auf $\mathbb{Q}$ bis auf Äquivalenz nur *einen* solche gibt, den gewöhnlichen Absolutbetrag, ist $|2|_v > 1$ für alle archimedischen v. Für $\mathbb{Q}$ besteht die Produktformel mit dem gewöhnlichen Betrag und den p-adischen Beträgen mit der Normierung $|p|_p = 1/p$ (es genügt, $x = -1$ und $x = p$ zu betrachten, und das ist trivial). Für $K = k(t)$, den rationalen Funktionenkörper in der Unbestimmten t über k, ist es leicht, eine Produktformel aufzustellen für das System derjenigen Bewertungen von K, die auf k trivial sind (im Kern ist das die Aussage, daß eine rationale Funktion auf der projektiven Geraden ebensoviele Nullstellen wie Pole hat); die Restkörper sind dann die endlichen Erweiterungen von k. Eine Produktformel geht, nach allgemeinen Sätzen über Bewertungsfortsetzung, auf endliche Erweiterungen über; genauer: gilt eine Produktformel für K und ein System S von Bewertungen von K, dann auch für die endliche Erweiterung L/K und das System der Fortsetzungen der Elemente von S auf L, bei geeigneter Normierung.

Hiernach sieht man, daß die beiden oben genannten Klassen von Körpern bei der sachgemäßen, bewertungstheoretischen Definition von „globaler Körper" in der Tat solche sind; schwierig ist der Nachweis, daß es keine weiteren gibt[1]. Es zeigt sich damit ferner, daß in beiden Fällen *alle* nichtarchimedischen Beträge endlichen Restkörper haben, und daß beide Male das System *aller* Bewertungen in der Formel vertreten ist. Es ist leicht, Körper zu konstruieren, die für zwei verschiedene Systeme von Beträgen Produktformeln haben (man nehme $k(t_1,t_2)$); aber solche sind nicht global.

Als „lokale" Körper sind dann sachgemäß die Komplettierungen der globalen nach ihren verschiedenen Bewertungen zu definieren; das entspricht auch dem Geist von „Tate's thesis" **[T]**, zu deren Verdiensten ja gehört, daß archimedische und nichtarchimedische Komplettierungen nach denselben Prinzipien behandelt werden. Als lokale Körper erweisen sich dann im Zahlkörperfall $\mathbb{R}$, $\mathbb{C}$ und die p-adischen Körper, d.h. die endlichen Erweiterungen von $\mathbb{Q}_p$; im Funktionenkörperfall die endlichen Erweiterungen eines Potenzreihenkörpers k((t)) bei endlichem k. Manche Autoren nehmen aber die archimedischen Komplettierungen, die ja keine natürliche arithmetische Struktur besitzen, von den lokalen Körpern aus [2].

1 Die einzige Referenz, die ich kenne, (außer der Originalarbeit von Artin und Whaples), ist das Buch **[A]** von Artin (darin Kapitel 12).

2 Ich habe nicht herausfinden können, wer zuerst den Ausdruck „globaler Körper" benutzt hat. Er scheint im Artin-Tate-Seminar über Klassenkörpertheorie Anfang der 50er Jahre verwendet worden zu sein (wie aus der 16 Jahre später publizierten Ausarbeitung hervorgeht). In Hasses frühen Arbeiten kommt er, soweit ich sehe, gar nicht vor; noch in seiner „Zahlentheorie" (1949) zieht er vor, „im Großen" und „im

Wo in der Zahlentheorie von „lokal“ die Rede ist, sind nicht die bloßen Lokalisierungen der Dedekindringe gemeint, sondern ihre Komplettierungen. Nach einem Primideal P lokalisieren bedeutet, alle Teilbarkeitsverhältnisse auf die P betreffenden zu reduzieren (schematheoretisch: das Spektrum wird auf zwei Punkte geschrumpft, einen offenen (=(0)) und einen abgeschlossenen (=(P)); der Preis dafür ist die nunmehr sehr vergrößerte Einheitengruppe, in die alles eingeht, was nicht zu P gehört, i.A. ohne strukturelle Auszeichnung. Diese „Verengung“ des Gesichtspunkts wird in der Komplettierung sozusagen auf die Spitze getrieben, die P-Teilbarkeit die einzige, die überhaupt noch erkennbar ist. Der Abschluß ist zugleich ein Ausschluß. Bildlich könnte man sagen: die Komplettierung verklebt das diskrete globale Objekt mit dem Leim des Kontinierlichen; nirgends besser zu veranschaulichen als beim Übergang von $\mathbb{Q}$ zu $\mathbb{R}$.[1] Sind p und q verschiedene rationale Primzahlen, kann die q-Bewertung zwar auf die Komplettierung $\mathbb{Q}_p$ fortgesetzt werden, aber das ist eine reine Existenzaussage, die auf der Wahl einer Transzendenzbasis von $\mathbb{Q}_p$ über $\mathbb{Q}$ beruht und (bisher wenigstens) für die Zahlentheorie bedeutungslos geblieben ist; und keinesfalls kann ein Körper bezüglich zweier nicht äquivalenter Bewertungen vollständig sein [2]. Auch verschiedene Komplettierungen in einem gemeinsamen Oberkörper zu vereinen, geht nur nichtkonstruktiv (man bilde das Tensorprodukt und teile ein maximales Ideal aus). Vollends „intransigent“ gegeneinander sind die Primkörper verschiedener Charakteristik. Daß es trotzdem, vermittelt durch den gemeinsamen überlagernden Ring $\mathbb{Z}$, algebraische Beziehungen zwischen ihnen gibt, wie das Quadratische Reziprozitätsgesetz, ist mit gutem Grund eine unversiegliche Quelle des Staunens [3].

Der „Ertrag“ der Komplettierung ist nun ein zweifacher: der komplettierte Körper enthält einen großen über dem Grundkörper algebraischen Teil, und mit dem Henselschen Lemma und dem ihm verwandten p-adischen Newtonverfahren hat man sehr starke Mittel, um das Nullstellen- und Zerlegungsverhalten von Polynomen zu untersuchen; topologisch wird durch die Komplettierung (bei endlichem Restkörper) die Topologie lokal-kompakt, wodurch analytische Methoden ins Spiel gebracht werden können; auf linearen Gruppen ein Haarsches Maß (so die Interpretation von Eulerfaktoren als p-adische Integrale, dem Ausgangspunkt von Tates thesis).

Das bringt uns zur sichtbarsten (aber nicht einzigen) raison d' être der Lokalisierungen in der Zahlentheorie. Viele globale Begriffsbildungen und Probleme habe lokale Analoga, und es ist eine natürliche Strategie, aus den lokalen Informationen globale zu ziehen. Die lokalen Situationen sind, aus den eben genannten Gründen, sehr viel einfacher zu

---

Kleinen“ statt „global“ und „lokal“ zu sagen (S.418 in der dritten Auflage 1969). Auch in Artins oben genanntem Buch fehlen die heute so geläufigen Bezeichnungen; Weil in seiner „Basic Number Theory“ schreibt „**A**-field“ statt „globaler Körper“. Aber spätestens seit Cassels-Fröhlich (1967) ist er durchgesetzt.

1 Wer es noch nicht weiß, mache sich klar, daß $\mathbb{Q}$ bezüglich der Betragstopologie total unzusammenhängend ist.

2 Siehe Bourbaki **[B]** , Ex. 16d auf S.468. Von der Wahl von Transzendenzbasen hängt übrigens auch die Einbettbarkeit der lokalen Körper in $\mathbb{C}$ ab, die allerdings manchmal nützlich ist.

3 Daß das quadratische Restverhalten von p mod q dem von q mod p reziprok ist, hat etwas Magisches, ähnlich wie Quantenkopplung: zwei Objekte, die „voneinander nichts wissen können“, stehen dennoch in einer „prästabilierten“ Beziehung.

behandeln; hinzu kommt oft, daß die unendlich vielen lokalen Strukturen, die aus *einer* globalen hervorgehen, fast alle von gleichförmiger und leicht zu beschreibender Natur sind; nur endlich viele sind „kritisch“. Der einfachste Fall ist nun der, daß eine Eigenschaft E global vorliegt genau dann, wenn dies überall lokal der Fall ist; man sagt dann, daß E einem „Lokal-Global-Prinzip“ oder „Hasse-Prinzip“ genügt, oder einfacher: E ist eine lokale Eigenschaft. Der Schluß vom Globalen aufs Lokale ist in aller Regel trivial; die entscheidende Frage geht auf den Rückschluß. Etwas allgemeiner kann man fragen, ob ein globales Bestimmungsstück durch seine lokalen Analoga determiniert wird. In manchen Fällen ist es möglich, die Abweichung von lokaler Determination, sozusagen das „globale surplus“, in einem Objekt sui generis mathematisch dingfest zu machen; Urbild sind hier die Funktoren der algebraischen Topologie, welche zum Beispiel die Nicht-Lokalität der Eigenschaft „einfach zusammenhängend“ durch die Fundamentalgruppe und die globale Nicht-Trivialität von (lokal trivialen) Vektorbündeln durch K-Gruppen „mißt“[1]. Ein anderer Aspekt der Lokal-Global-Beziehungen eröffnet sich, wenn man ein globales (algebro-geometrisches) Objekt mit allen zugeordneten lokalen Objekten gleichzeitig gewissermaßen konfrontiert, indem man es in deren (restringiertes) Produkt diagonal einbettet. Hier entsteht die Frage, „wie groß“ das globale Objekt im adelischen ist, präzisierbar durch schwache oder starke Approximation, bei linearen Gruppen auch die Tamagawazahl. Schließlich kann man die Analyse des Globalen durch das Lokale umkehren mit der Frage nach der Synthese: wann kommt eine Familie lokaler Objekte ein *einem* globalen Objekt her? Erst wenn man das verstanden hat, so werden wir an Hauptbeispielen sehen, hat man die Sache selbst verstanden; erst dann kann es eine *Klassifikation* der globalen Objekte geben.

4

Lokal-Global-Prinzipien finden sich in der Algebra lange vor aller Zahlentheorie. Sei R ein kommutativer Ring mit 1; für jedes Primideal P besteht ein kanonischer Morphismus $R \to R_P$. Das einfachste Lokal-Global-Prinzip bezieht sich auf Elemente von R und sagt, daß Gleichheit eine lokale Eigenschaft ist; man kann das ausdrücken durch die Injektivität der Abbildung

$$R \quad \to \quad \Pi_P \; R_P$$

(Produkt über alle P). Eine weitere lokale Eigenschaft von Elementen ist die, invertierbar zu sein; unter der obigen Abbildung ist also $R^\times$ das Urbild von $\Pi_P \; R_P{}^\times$.

Eine lokale Eigenschaft von R-Moduln ist es, der Nullmodul zu sein; eine Folgerung ist: gilt $N \subset M$, so ist $N = M$ genau dann, wenn $M_P = N_P$ für alle P ist. Ein Morphismus

1 Hier zeigt sich ein Unterschied zwischen der topologischen und der algebraisch-zahlentheoretischen Situation: in jener ist das Lokale (eine offene Kugel eines euklidischen Raums) tatsächlich trivial, in dem Sinn wenigstens, daß die wichtigsten Funktoren dafür verschwinden; in dieser aber nur „wesentlich einfacher“ und keineswegs immer trivial. Dahinter steht, daß die Grundobjekte der modernen Topologie, die Mannigfaltigkeiten, aus dem Lokalen aufgebaut werden, in der Zahlentheorie das Lokale dagegen aus dem Globalen abgeleitet wird. Für die Synthese kann man sich die Elemente aussuchen, bei der Analyse ist man von der Sache abhängig. Übrigens hat sich die Algebra in der Schematheorie auch das *glueing* der Topologen angeeignet.

$f: M \to N$ von R-Moduln ist injektiv (surjektiv, bijektiv) genau dann, wenn dies für alle $f_P: M_P \to N_P$ gilt. Man beachte aber: Isomorphie von Moduln ist keine lokale Eigenschaft; nur die Eigenschaft eines bestimmten f, ein Isomorphismus zu sein, ist lokal. „Flach" ist eine lokale Eigenschaft von Moduln, „frei" aber nicht. Unter den strukturellen Eigenschaften der Ringe sind lokal „Krull-Dimension = 1" und „ganz abgeschlossen" (letzteres nur für Integritätsbereiche); nicht lokal sind etwa „noethersch", „artinsch" oder „nullteilerfrei" (man nehme ein unendliches Produkt von Körpern). Das sind natürlich nur Kostproben; hier wünscht man sich Metatheoreme: Eigenschaften von Eigenschaften, die notwendig oder hinreichend für Lokalität sind. Die am wenigsten lokale Eigenschaft eines Ringes ist zweifellos die, ein lokaler Ring zu sein [1].

Wir nähern uns der Arithmetik, indem wir nach einem Begriff von Ganzheit fragen; sei jetzt R nullteilerfrei mit Quotientenkörper K. Wir könnten die Elemente von R für ganz erklären und hätten dann wenigstens ein Lokal-Global-Prinzip für Ganzheit, insofern

$$R = \bigcap R_P$$

ist (Durchschnitt über alle Lokalisierungen, gebildet in K; **[R]**, 3.17); doch sollte von Arithmetik nur gesprochen werden, wo eine brauchbare Idealtheorie vorliegt, und das ist in dieser Allgemeinheit nicht der Fall. Besser wird es schon, wenn wir R als Dedekindring annehmen; jetzt können wir von Primzerlegung sprechen, dem Ursprung aller Zahlentheorie. Jedes Primideal P induziert eine Bewertung v_P von K; es ist

$$R_P = \{ x \in K \mid v_P(x) \geq 0 \} ,$$

und die (nichttriviale!) letzte Gleichung wird zu der trivialen

$$R = \{ x \in K \mid v_P(x) \geq 0 \text{ für alle } P \} ,$$

worin der lokale Charakter von „Ganzheit" den deutlichsten Ausdruck findet. Bei den Dedekindringen begegnet uns eine erste „strukturell kontrollierte" Abweichung von einem Lokal-Global-Prinzip, nämlich bezüglich der Eigenschaft, ein Hauptideal zu sein. Bezeichnen Cl(R) die Idealklassengruppe von R und $K_0(R)$ die Grothendieckgruppe der endlich erzeugten projektiven R-Moduln, so gilt

$$K_0(R) \simeq Cl(R) \times \mathbb{Z} \ , \text{ speziell } K_0(R_P) \simeq \mathbb{Z}$$

(**[R]** § 36), weil die R_P als diskrete Bewertungsringe triviale Klassengruppen haben; demnach ist Cl(R) der Kern der Abbildung

$$K_0(R) \to \Pi_P \ K_0(R_P)$$

Ein weiteres Resultat soll erwähnt werden, welches die Konstitution globaler Objekte aus lokalen Vorgaben betrifft: Sei V ein endlich-dimensionaler K-Vektorraum, und für alle P sei X(P) ein R_P - Gitter in V; es gebe ein R-Gitter M derart, daß $M_P = X(P)$ für *fast alle* P gilt. Dann gibt es auch ein R-Gitter L mit $L_P = X(P)$ für *alle* P (**[R]** 4.22). Auf

1 Für einige Aussagen dieses Absatzes siehe **[AM]** oder **[R]** ; die übrigen sind einfache Übungen.

den ersten Blick scheint hier nicht viel geleistet, weil die Konklusion an fast allen Stellen vorausgesetzt wird. Aber die Voraussetzung besagt, intuitiv gesprochen, daß die Nenner der Koordinaten von R_P - Basen der X(P) bezüglich einer festgewählten K - Basis von V nicht beliebig groß werden, und eine solche Voraussetzung ist offensichtlich notwendig für die Konklusion; was der Satz leistet, ist eine Art Approximation für Gitter.

5

Ab jetzt bezeichne K einen Zahlkörper und M(K) die Mengen der Stellen von K; der Ausdruck „lokal“ bezieht sich im Folgenden immer auf die *Komplettierungen* K_v von K nach den v aus M(K). Einen möglichen Rahmen für Lokal-Global-Probleme bilden Funktoren F : {Erweiterungskörper L/K} → Mengen; man kann dann versuchen, Informationen über F(K) vermittels solcher über die $F(K_v)$ zu erhalten. Wir betrachten zuerst drei Beispiele, in denen die Werte F(L) selbst algebraische Strukturen tragen.

Wir rekapitulieren zunächst einige Grundbegriffe aus der Theorie der quadratischen Formen [1]. Eine solche wird, über dem beliebigen Körper k (mit chark ≠ 2), gegeben durch einen (endlich-dimensionalen) k - Vektorraum V mit einer symmetrischen Bilinearform B: $V \times V \to k$; es ist dann $q(x) = B(x,x)$ die zugeordnete Form, aus der B durch die Polarisationsformel

$$B(x,y) = 1/2\,(q(x+y) - q(x) - q(y))$$

zurückgewonnen werden kann; der zugehörige Begriff eines Morphismus von Formen (oder Räumen) ist klar. Man nennt q *isotrop,* wenn $q(x) = 0$ für ein $x \neq 0$ ist, sonst *anisotrop*; *total isotrop* bedeutet $q \equiv 0$ (und dann auch $B \equiv 0$). Die *hyperbolische Ebene* H ist der zweidimensionale Raum mit der Form $q(x,y) = xy$ (oder, äquivalent dazu, $x^2 - y^2$); ein *hyperbolischer Raum* ist eine orthogonale Summe von hyperbolischen Ebenen. Die fundamentale Strukturaussage ist: jeder quadratische Raum ist isomorph („isometrisch“) zu einer orthogonalen Summe aus einem total isotropen, einem hyperbolischen und einem anisotropen Raum; diese „Wittzerlegung“ ist eindeutig. Der Raum (oder die Form) heißt *regulär*, wenn der total isotrope Anteil (das Radikal) verschwindet. Die beiden natürlichen Hauptfragen sind: (1) welche Elemente von k werden durch eine gegebene Form dargestellt, (2) wie kann man die Formen über k klassifizieren?

Das Grundfaktum bezüglich der ersten Frage ist: eine (reguläre) Form ist universell (stellt alle Elemente von k dar) genau dann, wenn sie isotrop ist. Leicht zu beweisen ist dann: die Form q stellt die Zahl a dar genau dann, wenn die Form $q - ax^2$ isotrop ist (hier ist x eine Variable, die in q nicht vorkommt). Die Frage der Darstellbarkeit ist damit auf die nach Isotropie zurückgeführt. Für Zahlkörper (allgemeiner: globale Körper) k = K lautet die fundamentale Aussage einfach, daß Isotropie von Formen eine lokale Eigenschaft ist, explizit: eine (reguläre) Form q ist isotrop über K genau dann, wenn sie es über allen K_v ist. Dieser von Minkowski (für $K = \mathbb{Q}$) und Hasse (für allgemeine K) stammende Satz ist das am häufigsten genannte Beispiel für ein Lokal-Global-Prinzip, in dem auch die Bezeichnung „Hasse-Prinzip“ ihren Ursprung hat; der

1 Für alles hier Referierte siehe **[La]**.

einfachste Fall ist das Hasse-Prinzip für die Eigenschaft, ein Quadrat zu sein, was natürlich für $K = \mathbb{Q}$ trivial ist, aber schon nicht mehr, wenn nichttriviale Einheiten und Idealklassen vorhanden sind. Ein anderes Beispiel ist der Kreis $x^2 + y^2 = 3$ der keinen $\mathbb{Q}$-rationalen Punkt hat; der Beweis (man macht die Gleichung ganzzahlig und betrachtet sie mod 3) zeigt, daß auch kein 3-adischer Punkt existiert. Über nichtreellen K_v ist q isotrop, sobald dim B > 4 ; daher sind solche q genau dann isotrop über K, wenn sie es über allen reellen Komplettierungen sind. Es verdient hervorgehoben zu werden, daß der Satz von Hasse-Minkowski das globale Problem, ob eine gegebene Zahl durch eine gegebene Form dargestellt wird, algorithmierbar macht, indem die entsprechenden lokalen Probleme fast alle trivial und die restlichen systematisch zu behandeln sind (Stichworte: Quaternionenalgebren, Hilbertsymbol, Lemma von Hensel, quadratische Reziprozität).

Die Frage nach der Klassifikation reduziert sich sofort auf die anisotropen Formen, die man (wunderbarerweise) durch einen Funktor repräsentieren kann, dessen Werte *kommutative Ringe* sind. Die Isometrieklassen der quadratischen Räume bilden bezüglich der orthogonalen Summe und des Tensorprodukts einen kommutativen Halbring, der vermittels der Grothendieck-Konstruktion bezüglich der addiven Halbgruppe zu einem Ring wird; die Vielfachen von H erweisen sich als Ideal dieses Rings, und der Restklassenring nach diesem ist definitionsgemäß der *Wittring* W(k). Seine nichttrivialen Elemente entsprechen bijektiv den Isometrieklassen k-anisotroper Formen, also dem „interessanten“, für k spezifischen Bestand von Formen. Für die Komplettierungen der Zahlkörper ergibt sich $W(\mathbb{C}) = 0$ (weil es über $\mathbb{C}$ keine anisotropen Formen gibt), $W(\mathbb{R}) = \mathbb{Z}$ (vermöge der Signaturabbildung), und die $W(K_v)$ für endliche Stellen v können auf die Wittringe der endlichen Restklassenkörper zurückgeführt werden[1]; diese Ringe sind selbst endlich (mit vier Elementen für nichtdyadische v) und von sehr einfacher Struktur. Aus dem Satz von Hasse-Minkowski folgert man leicht, daß die Abbildung $W(K) \rightarrow \Pi_v\ W(K_v)$ injektiv ist; in Worten: zwei Formen haben denselben „anisotropen Kern“, wenn das überall lokal der Fall ist; speziell: die Eigenschaft, ein hyperbolischer Raum zu sein, ist lokal. Das Klassifikationsproblem läuft damit hinaus auf das „Syntheseproblem“: wann kommt eine Kollektion lokaler Formen (bis auf Isomorphie) von einer globalen? Diese Frage kann man vollständig beantworten; ich führe das aber hier nicht aus, weil es uns nötigen würde, tiefer in die Strukturtheorie einzusteigen, und verweise auf **[OM]**, § 72. Es sollte demnach möglich sein, in der exakten Seqenz (additiver Gruppen)

$$0 \quad \rightarrow \quad W(K) \quad \rightarrow \quad \Pi_v\ W(K_v) \quad \rightarrow \quad C \quad \rightarrow \quad 0$$

den Cokern C explizit zu beschreiben; was ich in der einschlägigen Literatur aber nicht gefunden habe [2] .

6

Ein formal gleichaussehendes, sogar einfacher zu handhabendes, aber doch bedeutend schwieriger zu gewinnendes Resultat erhält man für endlich-dimensionale einfache K-

1 Außer im dyadischen Fall, der sich aber mit ad-hoc-Argumenten behandeln läßt.
2 Für $K = \mathbb{Q}$ ergibt sich eine solche Sequenz leicht aus dem bei Lam S.174ff Bewiesenen.

Algebren, deren Zentrum K ist [1]. Das (über K gebildete) Tensorprodukt von zwei solchen Algebren ist wieder eine solche; man erhält also zunächst eine Halbgruppe von Isomorphieklassen. Erklärt man A und B für *ähnlich*, wenn es natürliche m, n gibt derart daß $M_n(A) \simeq M_m(B)$, bilden die Ähnlichkeitsklassen eine Gruppe, deren Einsklasse aus den vollen Matrixringen über K besteht; dies ist die *Brauergruppe* Br(K). Nach einem Satz von Wedderburn hat jedes A die Form $M_n(D)$ mit einem *Schiefkörper* D, und die Elemente von Br(K) entsprechen bijektiv den (Isomorphieklassen von) Schiefkörpern mit Zentrum K, genau wie der Wittring den anisotropen Formen. Die Funktoreigenschaft von Br ergibt sich daraus, daß für jedes A und jeden Erweiterungskörper L/K das Tensorprodukt von L und A eine zentral-einfache L-Algebra ist; man nennt L einen *Zerfällungskörper* von A, wenn dieses Produkt ein voller Matrixring über L wird, oder die Brauerklasse von A im Kern des Homomorphismus $Br(K) \to Br(L)$ liegt. Aus der Tatsache, daß es stets Zerfällungskörper gibt (zum Beispiel den algebraischen Abschluß von K), folgt, daß die K-Dimension von D eine Quadratzahl d^2 ist; man nennt dann d den *Schiefkörperindex* von A.

Für die Komplettierungen der Zahlkörper erhalten wir zunächst $Br(\mathbb{C}) = 0$ (über einem algebraisch abgeschlossenen L kann es keine endlich-dimensionalen Schiefkörper geben, weil jedes nicht in L liegende Element einen *kommutativen* Erweiterungskörper erzeugen würde); $Br(\mathbb{R})$ ist zyklisch von der Ordnung 2, wobei das nichttriviale Element durch den Hamiltonschen Quaternionenschiefkörper repräsentiert wird (das ist schon schwieriger und geht auf Frobenius zurück); wir schreiben diese Gruppe in der Form $(1/2)\mathbb{Z}/\mathbb{Z}$. Für die nichtarchimedischen Komplettierungen ist einheitlich (erstaunlicherweise, nicht einmal p=2 macht eine Ausnahme)

$$Br(K_v) \simeq \mathbb{Q} / \mathbb{Z} \ ;$$

die *Invariantenabbildung* inv_v, welche diesen Isomorphismus liefert, kann z.B. aus einer Realisierung einer zentral-einfachen K_v-Algebra als zyklisches verschränktes Produkt abgeleitet werden. Das Hauptresultat für Zahlkörper (bewiesen von Hasse-Brauer-Noether) ist eine exakte Sequenz

$$0 \quad \to \quad Br(K) \quad \to \quad \oplus\, Br(K_v) \quad \to \quad \mathbb{Q} / \mathbb{Z} \quad \to \quad 0 \ ,$$

wobei der zweite Pfeil die Summe der inv_v und der dritte einfach Summenbildung in $\mathbb{Q}/\mathbb{Z}$ ist[2]. Wie im Fall des Wittrings sind hier zwei fundamentale Tatsachen kodifiziert: die Injektivität von $Br(K) \to \oplus\, Br(K_v)$ besagt, daß ein globales A genau dann (über K) zerfällt, wenn dies über allen K_v der Fall ist; allgemeiner: A und B sind ähnlich, wenn sie es an allen Stellen sind. Für zyklische Algebren läuft dies hinaus auf den Hasseschen Normensatz. Die Exaktheit in der Mitte setzt uns hier instand, die Lösung des Syntheseproblems ohne weiteres anzugeben: eine Familie lokaler Invarianten kommt von einem globalen A her genau dann, wenn fast alle Mitglieder = 0 sind und die

1 Hier verweise ich auf **[R]**.

2 Man beachte, daß hier in der Mitte eine direkte *Summe* steht, bei den Wittringen ein *Produkt*. Eine K-anisotrope Form kann auch an unendlich vielen Stellen anisotrop sein (doch nur in kleinen Dimensionen; siehe **[CF]**, Ex.4); aber eine einfache Algebra hat nur endlich viele Verzweigungsstellen.

restlichen sich in $\mathbb{Q}/\mathbb{Z}$ zu Null summieren; das läuft hinaus auf einen Existenzsatz für zyklische Erweiterungen mit vorgebenenen lokalen Graden, den Satz von Grunwald-Wang. Der Schiefkörperindex von A ist dann das kgV der lokalen Indices. Man sieht, daß unser Hauptsatz in engster Beziehung zur Klassenkörpertheorie steht; in der Tat ist es möglich, für deren Aufbau die Algebrentheorie heranzuziehen. Der „quadratische" Teil der Brauergruppe, repräsentiert durch Quaternionen, spielt eine Rolle beim Beweis des Satzes von Hasse-Minkowski, da man gewisse ternäre und quaternäre Formen als Normformen solcher Algebren erhält [1].

7

Nach den Funktoren „Wittring" und „Brauergruppe" betrachten wir nun den einfachsten aller Funktoren, die Identität; einfach ist allerdings nur die Definition, logisch ist klar, daß er der schwierigste ist, weil wir nicht einen speziellen Aspekt der Körper isolieren, sondern diese sozusagen „mit allem, was sie sind" ins Auge fassen. Wir fragen also, inwieweit und wie K und einzelne Bestimmungsstücke von K durch die Gesamtheit der K_v mit ihren entsprechenden Bestimmungsstücken determinert sind; diese Gesamtheit, mit ihren Vielfachheiten, bezeichnen wir mit $\mathfrak{L}(K)$. Dies ist also eine *Folge* lokaler Körper; wir denken sie als mit den archimedischen beginnend, dann die 2-adischen, 3-adischen usw. Für eine Stelle v von $\mathbb{Q}$ erhält man die „v-adischen" Mitglieder von $\mathfrak{L}(K)$, indem man das Tensorprodukt von $\mathbb{Q}_v$ und K in seine direkten Faktoren zerlegt (oder äquivalent: ein erzeugendes Polynom von K über $\mathbb{Q}_v$ faktorisiert).

Die Antwort auf die erste Frage fällt überraschend aus: es gibt nicht-konjugierte K mit derselben Familie von Komplettierungen, darunter auch solche mit verschiedenen Klassenzahlen [2]. Allerdings haben solche stets eine gemeinsame galoissche Hülle, sind also immer nur in endlicher Anzahl vorhanden. Absolut galoissche K sind nach dem Satz von Bauer bereits durch die in ihnen enthaltenen Primideale ersten Grades bestimmt, also einen kleinen Teil der lokalen Information; dennoch ist auch in diesem Fall von Interesse, zu sehen, *wie* einzelne globale Informationen aus den lokalen hervorgehen. Fragen wir nun nach den durch $\mathfrak{L}(K)$ gegebenen Informationen, so ist an erster Stelle zu nennen das gesamte Zerlegungsgesetz der Erweiterung $K/\mathbb{Q}$, die unendlichen Stellen eingeschlossen. Durch diese ist der Einheitenrang von K gegeben; zur vollen Einheitenstruktur wird noch die Einheitswurzelzahl w(K) benötigt, welche einfach der ggT der entsprechenden lokalen Anzahlen ist (wenn alle K_v eine n-te Einheitswurzel enthalten, dann auch K; man betrachte das zugehörige Kreisteilungspolynom). Ferner ist natürlich der Grad n von K gegeben, zum Beispiel als Summe der $\mathbb{R}$-Dimensionen der archimedischen K_v . Sodann Differente und Diskriminante, als lokale Bildungen; weiteres werden wir unten bei der Besprechung der Zetafunktionen anführen.

Wir fragen nun nach der Eigenschaft, (absolut) galoissch zu sein, und ziehen dazu eine weitere Folgerung aus den Dichtigkeitssätzen heran: die Menge P(K) der rationalen Primzahlen, welche in K einen Primteiler ersten Grades haben, hat eine Dirichletsche Dichte $\geq 1/n$ mit Gleichheit *genau dann*, wenn K galoissch ist [3]. Also ist diese Frage

1 Siehe **[La]**, S.169 , **[OM]**, Ch.VI.
2 Beispiele bei **[Kl]**, S.240.
3 Siehe **[H]**, § 25.

lokal determiniert, und das ist erstaunlich, denn sie genügt keinem einfachen Lokal-Global-Prinzip: das Polynom $x^3 - x - 1$ definiert eine nicht galoissche Erweiterung K von $\mathbb{Q}$, aber alle K_v sind galoissch über den entsprechenden Grundkörpern $\mathbb{Q}_p$ (die Diskriminante ist –23, also hat 23 zwei Primteiler in K mit Komplettierungen der Grade 1 und 2 über $\mathbb{Q}_{23}$; die andern p sind unverzweigt, die entsprechenden K_v also zyklisch). Ist K galoissch, können wir weiter fragen, ob K abelsch ist, und hier ist der Befund ähnlich: nach dem Satz von Kronecker-Weber zusammen mit dem Bauerschen Satz ist K abelsch genau dann, wenn es eine Zahl m gibt derart, daß die Menge P(K), die jetzt mit der Menge der voll zerfallenden p zusammenfällt, ganz in einer Vereinigung von primen Restklassen mod m liegt, die die Einsklasse einer Faktorgruppe von $(\mathbb{Z}/m\mathbb{Z})^\times$ bilden [1]. Auch diese Eigenschaft ist also lokal determiniert, genügt aber nicht dem simplen Lokal-Global-Prinzip: man nehme für K den Zerfällungskörper eines Polynoms $x^3 - p$, p prim, mit der Galoisgruppe S_3. Alle $q \neq p, 3$ sind unverzweigt; für $p \equiv 1 \bmod 9$ sind p und 3 zerlegt (siehe z.B. **[Ma]**, Ex. 26e auf S.89), die Zerlegungsgruppen als echte Untergruppen von S_3 abelsch. Schließlich ergibt sich dasselbe Bild, wenn wir K als abelsch voraussetzen und fragen, ob K zyklisch ist: man findet leicht (z.B. unter biquadratischen K) Gegenbeispiele zum einfachen Lokal-Global-Prinzip; andererseits folgt aus dem Satz von Tschebotareff, daß K zyklisch ist genau dann, wenn es eine Primzahl p und einen Teiler v von p in K gibt, derart daß K_v über $\mathbb{Q}_p$ unverzweigt ist mit demselben Grad wie K über $\mathbb{Q}$; diese Eigenschaft ist also ebenfalls durch $\mathfrak{L}(K)$ determiniert. Die lokalen Galoisgruppen sind Untergruppen der globalen Gruppe, und in dieser ist jede Konjugationsklasse unendlich oft eine Frobeniusklasse; dennoch kann man nur schwache Rückschlüsse von den lokalen Gruppenstrukturen auf die globale erwarten, begrenzt schon dadurch, daß die lokalen Gruppen stets auflösbar sind.

Man bemerkt hier ein methodisches Problem, das Hervorhebung verdient: manches ist aus $\mathfrak{L}(K)$ ablesbar oder *berechenbar*, wie Grad, Diskrininante und Einheitenstruktur, anderes aber durch $\mathfrak{L}(K)$ - wenigstens vorerst - nur *determiniert*, wie die Eigenschaft, galoissch zu sein. Was man hier zur algorithmischen Entscheidung der Frage benötigte (gesetzt den Fall, sie würde je einmal virulent), wäre eine endliche Schranke S, derart, daß die Dichte der vollzerlegten p schon dann > 1 ist, wenn dies für die Dichte unterhalb von S gilt. Für die Eigenschaften, abelsch oder zyklisch zu sein, überlegt man sich leicht ähnliche Kriterien.

Nur kurz gehen wir auf das Syntheseproblem ein, das hier den „harten Kern“ der Sachen bildet: wann ist eine Familie $\mathfrak{L}$ von lokalen Körpern ein $\mathfrak{L}(K)$? Eine Reihe von notwendigen Bedingungen ist leicht anzugeben und ergibt sich ja aus dem oben Erörterten: nur endlich viele sind archimedisch, fast alle unverzweigt, für alle Stellen v von $\mathbb{Q}$ hat die Summe der $\mathbb{Q}_v$ -Dimensionen der vorkommenden Erweiterungen von $\mathbb{Q}_v$ denselben konstanten Wert; Vorgabe von Grad und Verzweigung lassen bekanntlich nur noch endlich viele Möglichkeiten für das gesuchte K [2]. Ob K, falls existent, galoissch

1 Es gibt aber *nicht galoissche* K, die ein „quasiabelsches“ Zerlegungsverhalten haben; siehe **[Kl]** S.39.

2 Es lohnt sich vielleicht, hier etwas näher hinzusehen. Die genannten Vorgaben lassen zunächst nur endlich viele Möglichkeiten für die verzweigten Komplettierungen, einfach weil ein lokaler Körper nur endlich viele Erweiterungen von gegebenem Grad hat. Es bleiben dann, rein kombinatorisch, immer noch unendlich viele Möglichkeiten für die Verteilung der Restklassengrade an den unverzeigten Stellen. Die globale Restriktion ist hier in letzter Instanz der Gitterpunktsatz, durch den die Koeffizienten erzeugender Polynome beschränkt werden können (siehe den Beweis bei **[L]**, S.122). Was wir gern hätten, ist nicht

ist, ist durch $\mathfrak{L}$ determiniert; mit dem Bauerschen Satz können wir schließen, daß wir „nur noch“ wissen müssen, ob eine gegebene Menge von Primzahlen (bis auf eine Menge der Dichte 0) die Form P(K) für ein galoissches K hat. Das aber ist nicht viel weniger als das große und immer noch unbewältigte Problem einer nichtabelschen Klassenkörpertheorie. Immerhin können wir eine „endliche Approximation“ konstatieren: wir sagen, daß ein p-adischer Körper K_p / $\mathbb{Q}_p$ durch den Zahlkörper K *realisiert* wird, wenn $K_p = K\,\mathbb{Q}_p$. Seien nun für endlich viele verschiedene Primzahlen p-adische K_p vorgegeben, alle vom Grad n; dann existiert ein Zahlkörper K vom Grad n, derart daß jedes dieser K_p durch einen zu K konjugierten Körper realisiert wird. (Sind endlich viele erzeugende Polynome mit rationalen Koeffizienten vorgegeben, wende man den Approximationssatz koeffizientenweise an und erhält ein rationales Polynom, das alle gegebenen simultan approximiert. Jetzt verwende man das Lemma von Krasner; Details in **[L]**, S.44). Sind die Erweiterungen K_p /$\mathbb{Q}_p$ zyklisch, kann man auch ein zyklisches K/$\mathbb{Q}$ finden (Satz von Grunwald-Wang); das folgt allerdings nicht aus diesem simplen Argument, sondern erfordert Klassenkörpertheorie. Wie beim Wittring und der Brauergruppe können also *endlich* viele lokale Vorgaben durch ein globales Objekt simultan realisiert werden (und zwar auf unendlich viele Weisen; das folgt von selbst aus der Aussage); anders als bei jenen kennen wir aber nicht die *constraints*, welchen eine *Gesamtheit* von lokalen Objekten unterliegen muß, wenn sie globaler Herkunft sein soll.

Eine eigene Betrachtung verdient das Lokal-Global-Prinzip in der Klassenkörpertheorie, auf die uns ja schon die Brauergruppe verwiesen hat. Bekanntlich hat zunächst Hasse die lokale Klassenkörpertheorie aus der globalen abgeleitet, dann haben Schmidt und Chevalley die lokale Theorie unabhängig von der globalen entwickelt, schließlich hat der letztere gezeigt, wie sich vermittels des Idelbegriffs die lokale Theorie zum Aufbau der globalen heranziehen läßt; damit hat, wie Hasse **[HH]** schreibt, das Lokal-Global-Prinzip in der Klassenkörpertheorie „Wurzeln geschlagen“. Die idelische Formulierung ernöglicht in der Tat den denkbar einfachsten Lokal-Global-Übergang am zentralen Punkt: das globale Normrestsymbol ist das Produkt der lokalen Symbole. Die gleichzeitig ins Spiel gebrachte Kohomologietheorie ermöglicht einen zweiten glatten Übergang: die Kohomologiegruppen der Idelgruppe sind Produkte lokaler Kohomologiegruppen (freilich gilt das nicht mehr für die der Idel*klassen*gruppe, die jetzt auf der einen Seite des Reziprozitätsgesetzes steht). Weiter ermöglichte die kohomologische Fassung eine vollständige Ablösung des beteiligten gruppentheoretischen Mechanismus von den spezifisch arithmetischen Sachverhalten, nämlich im Begriff der Klassenformation, der die lokale und die globale Theorie als Spezialfälle enthält [1]; es bleiben dann „nur noch“ die Axiome einer solchen zu verifizieren, die dann Reziprozitätsgesetz und Existenzsatz automatisch nach sich ziehen.[2]

---

bloß numerische, sondern strukturelle Restriktion.

1 Eine substantielle Vereinfachung des gruppentheoretischen Apparats bringt Neukirchs „abstrakte Klassenkörpertheorie“, die mit H^0 und H^1 auskommt (**[N]**); dahinter steckt, daß man wichtige Beweisschritte auf den zyklischen Fall reduzieren kann, die Kohomologie zyklischer Gruppen aber periodisch mit der Periode 2 ist.

2 Vom modernen „strukturellen“ Gesichtspunkt aus ist dies die durchsichtigste Präsentation der Klassenkörpertheorie; schwerlich ist es der natürliche Zugang. Man kann auch nicht behaupten, daß die Beweise insgesamt sich verkürzt hätten. Siehe die Bemerkungen in **[J]**, S.106.

Wir gehen jetzt über zu Varietäten. Wie beim Spezialfall der quadratischen Formen gilt die erste Frage der Existenz rationaler Punkte, was wir unter dem hier eingenommenen „lokal-global-Gesichtspunkt“ so formulieren können: gegeben sei eine Familie **F** von Varietäten; man sagt, daß für **F** das Hasse-Prinzip gilt, wenn wenn jedes Mitglied X von **F** einen rationalen Punkt hat, sobald dies überall lokal gilt, in einer Formel:

$$\Pi_v \; X(K_v) \neq \emptyset \quad \Rightarrow \quad X(K) \neq \emptyset \; .$$

Man kann die Definition natürlich auch für einzelne X aussprechen; das Hasse-Prinzip gilt dann trivial, wenn $X(K) \neq \emptyset$ oder $X(K_v) = \emptyset$ für ein v ist. Wie die bisher erreichten Resultat suggerieren, ist es aber sachgemäß, von vornherein Familien zu betrachten; wenn das Prinzip für ein X gilt, dann sollte es auch für „genügend ähnliche“ Y gelten; was das genauer bedeuten soll, ist allerdings nicht ausgemacht.

Varietäten der Dimension 0 werden durch Polynome definiert, und hier gilt das Hasse-Prinzip: ein irreduzibles K-Polynom f von einem Grad > 1 kann nicht in allen K_v eine Nullstelle haben (**[J]**, Ex.5 S. 139; man braucht für den Schluß nur, daß f an *fast* allen v eine Nullstelle hat); wohl aber kann, wie wir hier erwähnen sollten, f überall reduzibel sein (z.B. wenn f ein galoissches Polynom mit nicht-auflösbarer Gruppe ist; Gegenbeispiele findet man auch leicht unter biquadratischen Körpern). Von besonderem Interesse ist die Gleichung $x^m = a$. Hier gilt das Hasse-Prinzip *beinahe*: ist die Gleichung lösbar in allen K_v, so auch in K, wenn der Körper der n-ten Einheitswurzeln über k, wo n den 2-Anteil von m bezeichne, über K zyklisch ist (**[AT]**, Ch.9, Thm.1); ohne diese Voraussetzung existieren Gegenbeispiele. Dafür braucht man für die conclusio auch hier nur, daß Lösungen *fast überall* existieren.

Glatte Kurven C vom Geschlecht Null sind birational äquivalent zur projektiven Geraden (für die das Hasse-Prinzip trivial gilt), und die Äquivalenz ist über K definiert, wenn C einen K-rationalen Punkt hat; das einfachste Beispiel ist die bekannte Parametrisierung des Einheitsreises. Hat C keinen K-Punkt, ist C ein Kegelschnitt, für den der Satz von Hasse-Minkowski gilt. Bei Kurven vom Geschlecht 1 stoßen wir auf das am häufigsten zitierte Gegenbeispiel zum Hasse-Prinzip, die *Selmerkurve*, die durch

$$3x^3 + 4y^3 + 5z^3 = 0$$

definiert ist; etwas älter ist das Beispiel von Lind und Reichardt,

$$2x^2 + 17y^4 - 1 = 0 \; ;$$

heute kennt man ganze Familien solcher Gegenbeispiele **([Si]**, S.316**).** Wie bei der Eigenschaft, ein Hauptideal in einem Zahlkörper zu sein, ist es hier möglich, die Abweichung vom Hasse-Prinzip durch eine Gruppe zu beschreiben; wir rekapitulieren die nötigen Definitionen. Eine *elliptische Kurve* E über dem Zahlkörper K ist eine glatte projektive Kurve vom Geschlecht 1 mit einem ausgezeichneten K-rationalen Punkt. Ein *prinzipal homogener Raum* für E/K ist eine glatte Kurve C über K mit

einer einfach transitiven, algebraischen und über K definierten Gruppenaktion $E \times C \to C$ von E; als „triviales“ Beispiel kann man $C = E$ nehmen. Der Begriff eines Isomorphismus solcher Räume ist klar. Es zeigt sich (entscheidend für unseren Zweck), daß C genau dann zum „trivialen“ Beispiel isomorph ist, wenn $C(K) \neq \emptyset$. Die Menge der Isomorphieklassen steht in Bijektion mit der Kohomologiegruppe $H^1(K, E)$ ($= H^1(Gal(K^{alg}/K,E))$) und hat daher selbst eine Gruppenstruktur (die auch rein geometrisch definiert werden kann); man nennt sie die *Weil-Châtelet-Gruppe* WC(E/K). Die nichttrivalen Elemente von $WC(E/K) \simeq H^1(K, E)$ entsprechen also, nach dem allgemeinen Prinzip der Galoiskohomologie, den Kurven über K, die über dem algebraischen Abschluß zu E isomorph werden. Analoge Definitionen und Sachverhalte bestehen für die Komplettierungen K_v , und weil alles funktoriell ist, gibt es einen Gruppenhomomorphismus

$$WC(E/K) \quad \to \quad \Pi_v \; WC(E/K_v),$$

dessen Kern die *Tate-Schafarewitsch-Gruppe* von E heißt und mit Ш(E/K) bezeichnet wird. Die nichttrivialen Elemente dieser Gruppe entsprechen also denjenigen C, die über allen K_v rationale Punkte haben, aber nicht über K, also denjenigen, die gegen das Hasse-Prinzip verstoßen. Damit ist die Abweichung von diesem gruppentheoretisch erfaßt und das „Lokal-Global-Verhalten“ der elliptischen Kurven zurückgeführt auf die Berechnung von Ш(E/K), wofür allerdings (noch) kein Algorithmus bekannt ist; ja sogar die Vermutung, daß diese Gruppe stets endlich ist, konnte bisher nur in Spezialfällen bewiesen werden. Zu diesen gehört das Beispiel der Selmerkurve; hier hat $Ш(E/\mathbb{Q})$ die Ordnung 9 (die Ordnung ist, wenn endlich, stets eine Quadratzahl). Die zugehörige elliptische Kurve E, für welche also die Selmerkurve ein nichttrivialer prinzipal homogener Raum ist, kann durch

$$60x^3 + y^3 + z^3 = 0$$

definiert werden; E ist die Jacobische der Selmerkurve (ein rationaler Punkt ist (0,1,-1)). Auch unter Kurven höheren Geschlechts findet man Beispiele, die das Hasse-Prinzip verletzen (**[CM]**).

Für allgemeine Varietäten ist unser Wissen vom Hasse-Prinzip so fragmentarisch, daß Swinnerton-Dyer die Frage, für welche Familien überhaupt sinnvoll ist, danach zu fragen, als Problem *sui generis* aufgeworfen hat (**[Sw]**, Question 3, S.8). Wie er gleichzeitig feststellt, ist die einzige bekannte *systematische,* im Prinzip überall anwendbare Methode die der „Brauer-Manin-Obstruktion“, die wir hier nur andeuten können [1]. Es sei K(X) der Funktionenkörper der *projektiven* Varietät X und A eine zentral-einfache K(X)-Algebra mit „guten Spezialisierungen“, d.h. jeder K-rationale Punkt x von X bestimmt durch Spezialisierung eine zentral-einfache K-Algebra A(x). Ebenso bestimmt jeder K_v-rationale Punkt x_v eine K_v - Algebra $A(x_v)$, jeder adelische Punkt $(x_v)_v$ also eine Familie $(A(x_v))_v$ lokaler Algebren; dabei sind deren lokale Invarianten (siehe oben (6)) fast alle = 0. Bezeichnen wir den Adelring von K mit

1 Siehe **[G]** und **[Sw]** für Näheres.

$\mathbf{A}(K)$[1], erhalten wir so eine Paarung

$$\mathrm{Br}(K(X)) \quad \times \quad X(\mathbf{A}(K)) \quad \to \quad \mathbb{Q}/\mathbb{Z} \ ,$$

$$(\mathrm{cl}(A) \ , \ (x_v)_v \ ) \quad \to \quad \Sigma_{\ v} \ \mathrm{inv}_v(A(x_v) \ .$$

Ist nun der adelische Punkt schon rational, also alle $x_v = x$, ist die Summe dieser Invarianten $= 0$, gemäß der exakten Sequenz in (6). Jeder rationale Punkt annihiliert damit ganz Br(K(X)), liegt also im Rechtskern dieser Paarung. Man sagt nun, daß X eine Brauer-Manin-Obstruktion hat, wenn dieser Rechtskern leer ist, aber $X(\mathbf{A}(K))$ nicht. Für projektive X ist $X(\mathbf{A}(K)) = \Pi_v X(K_v)$, die letzte Bedingung sagt also einfach, daß X überall lokale Punkte hat; ist aber der Rechtskern leer, dann auch X(K); das Vorliegen der Brauer-Manin-Obstruktion ist also eine *hinreichende* Bedingung dafür, daß X *nicht* das Hasse-Prinzip erfüllt. Im Gegensatz zum Augenschein ist nun dieser Rechtskern (in manchen Fällen wenigstens) der Berechnung zugänglich; für manche Klassen von Varietäten ist Brauer-Manin als einzige Obstruktion zum Hasse-Prinzip nachgewiesen, für andere wird dies vermutet, und es gibt Beispiele dafür, daß sie nicht die einzige Obstruktion ist.

Die bei den elliptischen Kurven benutzte Abbildung

$$H^1(K, E) \quad \to \quad \Pi_v \ H^1(K_v, E)$$

existiert auch, wenn statt E *lineare* algebraische K-Gruppen G betrachtet werden; nur hat man es dann statt mit Kohomologie*gruppen* mit punktierten Mengen zu tun, da die meisten G nicht kommutativ sind; immerhin kann man noch vom *Kern* einer solchen Abbildung sprechen. Unter recht allgemeinen Voraussetzungen beweisen Borel und Serre (**[BS]**) einen Endlichkeitssatz für diesen Kern; Serre konstruiert in **[SC]**, S.156ff ein Beispiel, in welchem der Kern nicht trivial ist. In vielen wichtigen Fällen aber ist die Abbildung injektiv, für einfach zusammenhängende halbeinfache H sogar bijektiv (**[Kn]**, S.257, **[PR]**, S.286). Wenn G die Automorphismengruppe einer Klasse algebraischer Objekte ist, dann bedeutet dies ein Hasse-Prinzip für solche Objekte: je zwei sind K-isomorph, wenn sie K_v-isomorph sind für alle v. Der Satz von Hasse-Minkowski tritt hier als Spezialfall auf; G ist dann die Automorphismengruppe einer Form.

Nächst der Frage nach rationalen Punkten ist die nach Isomorphie die natürlichste, und ebenso wie die Eigenschaft, rationale Punkte zu besitzen, nicht lokal ist, erweist sich dies auch für die Eigenschaft von Paaren X,Y von K-Varietäten, isomorph zu sein. Hier scheint die Theorie noch wenig entwickelt. Mazur **[M]** nennt Y einen *companion* [2] von X, wenn X und Y über allen K_v isomorph werden; sichtlich ist die Menge S(X/K) der (K-Isomorphieklassen von) *companions* ein Analogon zur Idealklassengruppe; sie „mißt“ die Abweichung der Eigenschaft, K-isomorph zu X zu sein, vom Hasse-Prinzip. Im Falle $K = \mathbb{Q}$ vermutet Mazur, daß für glatte projektive X die Menge $S(X/\mathbb{Q})$ stets endlich ist, und beweist dies für Kurven mit Geschlecht > 1 und Hyperflächen mit

1 Wir werden $\mathbf{A}(K)$ unten definieren.

2 Nach Mazur ein „neologism“; eine mir passend erscheinende Übersetzung ist mir nicht eingefallen; am ehesten ginge wohl „Begleiter“ (aber das klingt nicht symmetrisch genug).

Dimension > 2. Ein allgemeines Resultat (Thm.2) hat zur Voraussetzung die (vermutete) Endlichkeit der Tate-Schafarewitsch-Gruppen abelscher Varietäten (hier $Pic^0(X)$) sowie Endlichkeitsaussagen über die Gruppe der Zusammenhangskomponenten der lokal-algebraischen Gruppe Aut(V), deren Status noch unklar zu sein scheint. Unter den Kurven sind demnach die elliptischen die einzigen noch unbewältigten. Für die Selmerkurve aber gelingt es Mazur, alle *companions* aufzulisten: es sind, außer ihr selbst und ihrer schon angeführten Jacobischen, die drei weiteren Kurven $12x^3 + y^3 + 5z^3 = 0$, $15x^3 + 4y^3 + z^3 = 0$ und $3x^3 + 20y^3 + z^3 = 0$ (Thm.1). Keine von diesen hat also einen $\mathbb{Q}$-Punkt, alle haben Punkte über allen $\mathbb{Q}_v$, und alle haben dieselbe Jacobische.

9

Wir vereinigen nun die Gesamtheit der Komplettierungen K_v zum *Adelring*

$$\mathbf{A}(K) = \{(x_v) \in \Pi_v K_v \mid x_v \text{ ist v-ganz für fast alle v}\},$$

in welchen K diagonal eingebettet ist. In jedem einzelnen K_v ist K dicht nach Konstruktion, nach dem Approximationssatz sogar in jedem endlichen Produkt von Komplettierungen K_v oder, was dasselbe bedeutet, im Produkt *aller* K_v mit der *Produkttopologie*. In $\mathbf{A}(K)$ jedoch, mit der adelischen Topologie, deren typische offene Umgebungen der Null Produkte von offenen U_v in allen K_v sind, mit $U_v = O_v$ (der Bewertungsring von K_v) fast überall, ist K diskret; man sieht sofort, daß z.B. für $K = \mathbb{Q}$ die offene Menge

$$(0,1) \times \Pi_p \mathbb{Z}_p \subset \mathbf{A}(\mathbb{Q})$$

keine rationale Zahl enthält. Läßt man aber die reelle Komponente weg, so wird das Bild von $\mathbb{Q}$ in dem gesamten Rest, dem Ring $\mathbf{A}_f(\mathbb{Q})$ der *endlichen Adele*, dicht; das ist der *starke Approximationssatz*, den man aus dem chinesischen Restsatz ableiten kann [1]. Man kann aber statt der unendlichen auch eine beliebige andere Komponente streichen und erhält dasselbe Resultat; so sieht man leicht, daß z.B. in der Menge

$$(0,1) \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \ldots.$$

unendlich viele rationale Zahlen liegen; das wird manchmal auch der *sehr* starke Approximationssatz genannt (und ist *keine* Folgerung aus dem Restsatz allein). Analoge Aussagen gelten für alle Zahlkörper. In gewissem Sinne ist also K eine *maximale* diskrete Untergruppe von $\mathbf{A}(K)$; das werden wir noch präzisieren.

Eine K-Varietät X hat *schwache Approximation*, wenn X(K) in dem Produkt aller $X(K_v)$ mit der Produkttopologie dicht ist; der Approximationssatz sagt also, daß die Varietät $X = G_a$ schwache Approximation hat (und, wie man leicht folgert, auch G_m).

1 Es ist instruktiv, den allgemeinen Approximationssatz (Abschnitt 2) mit dem chinesischen Restsatz zu vergleichen (etwa in einem Dedekindring R). Der Restsatz liefert Approximation von Elementen von R durch ebensolche, an endlichen vielen vorgegebenen endlichen Stellen; der Approximationssatz würde hier nur Approximation durch Elemente von Quot(R) liefern. Dafür ist er auch auf archimedische Stellen anwendbar.

„Starke Approximation“ bezieht sich auf das adelische Objekt $X(\mathbf{A}(K))$, das man auch als restringiertes Produkt der $X(K_v)$ bezüglich der Teilmengen $X(O_v)$ einführen kann. X hat *starke Approximation*, wenn $X(K)$ dicht ist in $X(\mathbf{A}_f(K))$, wobei $\mathbf{A}_f(K)$ wie für $K = \mathbb{Q}$ der Ring der endlichen Adele ist [1] ; der starke Approximationssatz sagt also, daß $X = G_a$ starke Approximation hat. Für projektive X fallen starke und schwache Approximation zusammen, weil dann $X(K_v) = X(O_v)$ ist; man beachte, daß dann auch X(K) (sofern unendlich) nicht mehr diskret in $X(\mathbf{A}(K))$ ist, weil diese Menge kompakt ist. Schwache Approximation hängt nur von der birationalen Äquivalenzklasse von X ab und setzt sich fort auf Produkte; daraus folgt, daß affine und projektive Räume schwache Approximation haben, aber auch K-rationale Varietäten, z.B eine glatte projektive Quadrik mit einem K-rationalen Punkt (denn eine solche ist K-birational äquivalent zu einem projektiven Raum). Weitere Beispiele sind glatte Durchschnitte von Quadriken, Châtelet-Flächen und glatte kubische Hyperflächen, doch nur unter einschränkenden Bedingungen an Dimension und Grad; sind diese nicht erfüllt, gibt es Gegenbeispiele. Elliptische Kurven E sind Nicht-Beispiele, selbst wenn man von dem oben betrachteten (sozusagen extremen) Fall absieht, in welchem das Hasse-Prinzip verletzt ist. Die K-Punkte von E bilden stets eine „dünne“ Teilmenge von E, und darum gibt es zu jeder endlichen Stellenmenge von K eine endliche, zur ihr disjunkte Menge S, derart daß E(K) nicht dicht ist im Produkt der $E(K_v)$, $v \in S$; Analoges gilt für abelsche Varietäten (**[SG]**, Ex.4, S.20 und Satz 3.5.3)[2]. Auch für schwache Approximation kann man eine „Brauer-Manin-Obstruktion“ definieren. Im Ganzen ist unser Wissen hier ähnlich fragmentarisch wie beim Hasse-Prinzip für rationale Punkte; doch ein allgemeines Resultat von Minchev scheint darauf hinzuweisen, daß schwache Approximation Ausnahmecharakter hat: ist X projektiv und glatt, $X(K) \neq \emptyset$ und die étale Fundamentalgruppe über dem algebraischen Abschluß nichttrivial, dann hat X keine schwache Approximation [3] .

Gute Resultate besitzen wir jedoch für lineare algebraische Gruppen $X = G$ [4], dank der gut verstandenen Strukturtheorie dieser Objekte. Zunächst ziehen wir die *Levizerlegung* $G = HR_u(G)$ von G heran (ein semidirektes Produkt einer reduktiven Gruppe H mit dem unipotenten Radikal $R_u(G)$ von G), die das Problem auf den reduktiven Fall zurückführt, denn das Radikal ist als unipotente Gruppe isomorph zu einem affinen Raum. Alle halbeinfachen einfach zusammenhängenden G haben schwache Approximation (S.415); aber auch z.B. $G = GL_n$, als offene Teilmenge eines affinen Raums. Für jedes zusammenhängende G gibt es eine endliche Menge S endlicher Stellen, derart daß G außerhalb von S schwache Approximation hat, d.h. G(K) ist dicht im Produkt der restlichen $G(K_v)$; insbesondere ist G(K) stets dicht im Produkt der $G(K_v)$ für $v|\infty$ (S.415). Der Abschluß von G(K) im Produkt aller $G(K_v)$ ist ein Normalteiler von endlichem Index, mit abelscher Faktorgruppe, welche ein Maß für die Abweichung von der schwachen Approximation darstellt (S.421). Für den Norm-Eins-Torus G = T der

1 Es ist möglich (und sinnvoll), endliche Mengen von Primstellen aus der Betrachtung auszuschließen; das soll hier ad hoc gehandhabt werden; präzise Definitionen in **[PR]**, Kap.7.

2 Jedoch ist $E(\mathbb{Q})$ stets dicht in $E(\mathbb{R})$, wenn der Rang > 0 ist, weil $E(\mathbb{R})$ ein Kreis ist oder disjunkte Vereinigung von zwei Kreisen; im Einklang mit einer allgemeinen Vermutung von Mazur **[MR]**. Man kann hier nicht $\mathbb{R}$ durch ein $\mathbb{Q}_p$ ersetzen!

3 Alles in diesem Absatz Referierte stammt aus **[Ha]**.

4 Alles im Rest dieses Abschnitts Referierte stammt aus **[PR]**; Seitenzahlen beziehen sich auf dieses Buch. Man findet dort auch auch das Vokabular aus der Strukturtheorie, das wir hier ohne Erklärung benutzen müssen. Eine knappe, aber sehr klare Übersicht bietet **[Kn]**.

Erweiterung $\mathbb{Q}(\sqrt{-1}, \sqrt{2})/\mathbb{Q}$ beispielsweise kann man zeigen, daß $T(\mathbb{Q})$ nicht dicht in $T(\mathbb{Q}_2)$ ist und sein Abschluß den Index 2 in dieser Gruppe hat (S.412f). Eine reduktives G hat starke Approximation genau dann, wenn G einfach zusammenhängend und kein $G(K_v)$ für archimedisches v kompakt ist (S.427); Beispiele sind SL_n und allgemeiner $SL_n(D)$, wo D ein über K zentraler Schiefkörper ist (hier muß, damit die zweite Bedingung erfüllt ist, $n > 1$ sein, falls $[D:K] = 4$ und D an einer reellen Stelle von K verzweigt ist; denn für den Hamiltonschen Quaternionenschiefkörper **H** ist $SL_1(\mathbf{H}) = SO(3)$). Die multiplikative Gruppe $G = G_m$ ist reduktiv, aber nicht einfach zusammenhängend (alle Morphismen $x \rightarrow x^n$ sind Isogenien $G_m \rightarrow G_m$), hat demnach (wie allgemeiner GL_n) keine starke Approximation, was man sich für $K = \mathbb{Q}$ klar machen sollte; z.B. enthält die offene Menge

$$(5 + 8\,\mathbb{Z}_2) \times \mathbb{Z}_3^{\times} \times \mathbb{Z}_5^{\times} \times \ldots.$$

von $G_m(\mathbf{A}_f(\mathbb{Q})) = \mathbf{A}_f(\mathbb{Q})^{\times}$ keinen rationalen Punkt. Die additive Gruppe hat starke Approximation, obwohl sie ebenfalls nicht halbeinfach ist, aber sie ist auch nicht reduktiv und fällt damit nicht unter den Satz!

10

Schwache oder starke Approximation sind „Maße“ dafür, wie „groß“ G(K) in $G(\mathbf{A}(K))$ ist. Auf direkterem Wege kann man diese Frage angehen, indem man die Haarschen Maße heranzieht, welche die $G(K_v)$ und damit auch $G(\mathbf{A}(K))$ als lokalkompakte Gruppen tragen, und die man aus einer invarianten Differentialform höchsten Grades dim(G) auf G konstruieren kann. G(K) ist eine diskrete Untergruppe von $G(\mathbf{A}(K))$, so daß man Reduktionstheorie treiben und nach einem Fundamentalbereich für die Operation von G(K) auf $G(\mathbf{A}(K))$ sowie dessen Volumen fragen kann. Beschränken wir uns (nur der Einfachheit halber) auf $K = \mathbb{Q}$: Es ist nicht allzuschwer, zu zeigen, daß diese Reduktionstheorie „parallel“ läuft zu der klassischen, nämlich von $G(\mathbb{Z})$ auf $G(\mathbb{R})$; explizit: genau dann ist $G(\mathbf{A}(K))/G(K)$ kompakt (hat endliches Volumen), wenn das Entsprechende für $G(\mathbb{R})/G(\mathbb{Z})$ gilt (**[PR]** S.262). Notwendige und hinreichende Kriterien sind: für Kompaktheit: der reduktive Teil der Zusammenhangskomponente von G ist anisotrop über $\mathbb{Q}$; für endliches Volumen: die Zusammenhangskomponente hat keinen nichttrivialen über $\mathbb{Q}$ definierten Charakter (S.260). Die additive Gruppe G_a erfüllt das Kriterium für Kompaktheit (der reduktive Teil ist trivial). Aus der expliziten Beschreibung des Fundamentalbereichs (**[Ko]**, S.195) ersieht man, daß $\mathbf{A}(K)/K$ ein endliches Produkt von Kreisgruppen ist mit dem Produkt aller O_v ist ; weil die letzteren keine diskreten Untergruppen enthalten, sieht man, daß K eine *fast maximale* diskrete Untergruppe von $\mathbf{A}(K)$ ist, d.h. von endlichem Index in jeder diskreten Obergruppe. Die multiplikative Gruppe, und allgemeiner GL_n, genügen nicht dem Kriterium für Endlichkeit (det ist ein Charakter $GL_n \rightarrow GL_1 = G_m$); SL_n hat endliches Kovolumen, ist aber nicht kokompakt. Nichttriviale Beispiele für Kokompaktheit bieten die Norm-Eins-Gruppen von Schiefkörpern; das einfachste Beispiel sind die Hamiltonschen Quaternionen über $\mathbb{Q}$.

Ist das Kovolumen endlich, stellt sich die Frage nach seinem Wert, wozu natürlich eine sachdienliche Normierung der lokalen Haarmaße auf den K_v $(= G_a(K_v))$ zugrundegelegt

werden muß. Die „kanonische“ Wahl ist die, bei welcher dann, auf der adelischen Gruppe mit dem Produktmaß, die Fourierinversion in der einfachsten Form $f(-x) = f^{**}(x)$ gilt ($x \in \mathbf{A}(K)$, f geeignet, f^* die Fouriertransformierte). Für $K_v = \mathbb{R}$ ist dies das gewöhnliche Lebesguemaß, für $K_v = \mathbb{C}$ das zweifache des Lebesguemaßes (sachgemäß, weil *eine* komplexe Stelle von K einem *Paar* von Einbettungen in $\mathbb{C}$ entspricht), und für nichtarchimedische K_v dasjenige Maß, bei dem O_v das Volumen $\sqrt{d(K_v)}^{-1}$ annimmt (= 1 für fast alle O_v). Aus der schon herangezogenen expliziten Beschreibung des Fundamentalbereichs entnimmt man jetzt, daß $\mathbf{A}(K)/(K)$ das Volumen 1 hat: das Volumen eines Fundamentalbereichs für O_K auf dem unendlichen Teil von $\mathbf{A}(K)$, nämlich $\sqrt{|d(K)|}$, eine *geometrisch* definierte Größe, kürzt sich gegen das Produkt der lokalen Diskriminanten, Größen von *arithmetischer* Natur.

Für allgemeine G heißt das so berechnete Kovolumen von G(K) in $G(\mathbf{A}(K))$, falls endlich, die *Tamagawazahl* $\tau(G)$ von G [1]. Weil hat 1961 vermutet, und für einige Fälle bewiesen, daß für einfach zusammenhängende G stets $\tau(G) = 1$ ist, was bis 1989 nach und nach vollständig gezeigt werden konnte (**[PR]**, S.263). Welch ein erstaunlicher Sachverhalt sich hinter dieser bescheidenen Formel verbirgt, soll am einfachsten (nichtkommutativen) Beispiel der Gruppe $G = SL_2$ über $\mathbb{Q}$ illustriert werden: man zeigt zunächst (starke Approximation), daß ein Fundamentalbereich für die Operation von $G(\mathbb{Q})$ auf $G(\mathbf{A}(\mathbb{Q}))$ durch $F \times \Pi_p\, G(\mathbb{Z}_p)$ gegeben ist, wo F ein Fundamentalbereich für die Operation von $G(\mathbb{Z})$ auf der oberen Halbebene ist. Ein solcher ist allbekannt und hat das Volumen $\pi^2/6$. Die lokalen Volumina der $G(\mathbb{Z}_p)$ berechnen sich zu $1 - p^{-2}$, ihr Produkt ist also gleich dem Inversen von $\zeta(2) = \pi^2/6$! Eine Art Reziprozität zwischen den archimedischen und den diskreten Aspekten der Gruppe SL_2, die wir vorher schon für die additive Gruppe beobachtet haben, die aber doch hier (und erst recht in andern Fällen) von ungleich größerer Komplexität ist, und deren Faszination man sich schwer entziehen kann, grob gesagt: das Volumen eines Fundamentalbereichs der diskreten Gruppe $G(\mathbb{Z})$ auf der Liegruppe $G(\mathbb{R})$ „entspricht“ dem Produkt der Volumina der maximalen kompakten p-adischen Gruppen.

11

Die frappierendste Produktion globaler Information durch lokale findet bei den Zetafunktionen und ihren Verallgemeinerungen statt. Die Dedekindsche Zetafunktion $\zeta_K(s)$ des Körpers K enthält mit ihren Eulerfaktoren $(1 - NP^{-s})^{-1}$ (NP bedeute die Absolutnorm des Primideals P) zunächst nichts weiter als das Zerlegungsgesetz für die nichtarchimedischen Stellen von K, und auch dieses nicht vollständig, denn an den verzweigten Stellen bleibt noch Spielraum für die Verteilung der Verzweigungsindices. Weil wir aber *a priori* wissen, daß das durch „Gammafaktoren“ vervollständigte Eulerprodukt eine analytische Fortsetzung mit einer Funktionalgleichung besitzt, sind zunächst die Gammafaktoren eindeutig bestimmt (weil ein endliches Aggregat von solchen nicht selbst einer Funktionalgleichung genügen kann; für Details und eine sehr viel allgemeinere Aussage siehe **[Ro]**, S.414), damit auch die Zerlegung der unendlichen Stelle von $\mathbb{Q}$ [2]. (Ein analoges Argument zeigt übrigens, daß es auch auf endlich viele Eulerfaktoren nicht ankommt; und im (absolut) galoisschen Fall genügt zur

1 Auf die sog. konvergenzerzeugenden Faktoren brauchen wir hier nicht einzugehen.
2 Aber wie berechnet man die Gammafaktoren aus den Eulerfaktoren?

Identifikation von K (wie schon erwähnt wurde) sogar die Kenntnis der vollzerlegten rationalen p, einer Menge der Dichte 1/[K:ℚ].) Das ist immer noch viel weniger als die Kenntnis aller K_v ; dennoch sind durch die Zetafunktion die folgenden weiteren Bestimmungsstücke von K determiniert: die genaue Primzerlegung auch der verzweigten Stellen; die galoissche Hülle, der kleinste galoissche Teilkörper, die Diskriminante; die Einheitswurzelzahl w(K); die Isometrieklasse der Spurform $Sp_{K/\mathbb{Q}}(x^2)$, einer quadratischen Form der Dimension [K:ℚ] über ℚ ; siehe **[Kl]**, S.77ff für eine vollständigere Aufzählung, die auch im relativen Fall gültig ist, mit Beweisen. Als besonders bemerkenswert soll noch hervorgehoben werden: die Taylorentwicklung von $\zeta_K(s)$ an der Stelle $s = 0$ hat als Leitkoeffizient den Term $-h(K)R(K)/w(K)$ (in dem R(K) den Regulator bedeutet); da w(K) durch $\zeta_K(s)$ determiniert ist, so auch h(K)R(K); aber wegen der früher erwähnten Beispiele von Körpern mit gleichem $\mathfrak{G}(K)$, aber verschiedener Klassenzahl ist h(K) i.A. nicht determiniert, damit auch R(K) nicht, sondern eben nur das Produkt beider. Man denkt hier an den Brauer-Siegelschen Satz, daß log h(K)R(K) in geeigneten Folgen von Körpern K asymptotisch proportional zum Logarithmus der Diskriminante ist (siehe **[L]**, S.321), und fragt sich, ob dieses Produkt sich nicht einem einzigen Bestimmungsstück von K zuordnen läßt [1]. Bemerkenswert ist hier auch, daß mit w(K) und den unendlichen Stellen von K (oder auch der Nullstellenordnung von $\zeta_K(s)$ bei $s = 0$) die *Struktur* der Einheitengruppe sehr wohl festliegt; nur ihre numerische Invariante (der Regulator, ein Volumen) fehlt; wohingegen die additive Struktur mitsamt ihrem Volumen (der Diskriminante) lokal ohne weiteres ablesbar ist. Merkwürdig ist auch, daß die Einheitenstruktur, wenn die Leopoldt-Vermutung richtig ist, beim Lokalisieren sozusagen intakt bleibt (**[Wa]**, S.75), wie (trivialerweise) die additive Struktur, während die Klassengruppe sich auflöst [2].

Was hier aus der Theorie der Zahlkörper berichtet wurde, wird in analoger Weise auch für Varietäten erwartet. Ihre Zeta- und L-Funktionen, als Eulerprodukte definiert, also durch lokale Bestimmungsstücke, sollen in Werten, Leitkoeffizienten, Pol- und Nullstellenordnungen an speziellen Stellen globale numerische Invarianten der Varietäten enthalten. Das alles sind noch weitgehend Vermutungen, verbunden mit den Namen Beilinson, Bloch, Kato, Tate, Stark..., und um sie herum sind gewaltige Theoriegebäude entstanden, die hier auch nicht ansatzweise beschrieben werden können (siehe **[PRS]** für eine Reihe einführender Aufsätze). Nur die populärste soll genannt werden, die Vermutung von Birch und Swinnerton-Dyer: ist E eine elliptische Kurve über ℚ , so ist die Nullstellenordnung der Hasse-Weil-L-Funktion von E (der „interessante“ Faktor ihrer Zetafunktion) an der Stelle $s = 1$ gleich dem Rang der Gruppe E(ℚ); siehe **[Si]**, S.362f für eine instruktive Diskussion der Evidenz dafür. Es sollte hier vermerkt werden, daß es der Arbeit von Wiles et al. bedurfte, um sicherzustellen, daß die L-Funktion bei $s = 1$ überhaupt definiert ist! Und über alle Vermutungen hinaus kann vermutet werden, daß in jenen Funktionen manches verborgen ist, wovon wir noch gar nichts ahnen. „I do not believe that anything like the full story has yet been revealed“, so Swinnerton-Dyer (**[SW]** S.14).

1 Ich würde auch gern wissen, ob es noch weitere, prinzipiell nicht lokal determinierbare Bestimmungsstücke der Zahlkörper gibt (außerwesentliche Diskriminantenteiler?).

2 Im Lokalen sind übrigens additive und multiplikative Struktur via log und exp „virtuell“isomorph. Global sind sie „virtuell verwandt“ (freie ℤ-Moduln von bekanntem Rang), aber es gibt keine „kanonischen“ Abbildungen zwischen ihnen. Über die allgemeine „Inkompatibilität von Addition und Multiplikation“ siehe meinen Aufsatz **[K]**.

Es scheint „in der Natur der Sachen“ zu liegen, daß die „speziellen“ Stellen außerhalb des Konvergenzbereichs der definierenden Eulerprodukte liegen (dieser ist eine rechte Halbebene, in wohlbekannter Weise durch geometrische Invarianten definiert); obwohl natürlich durch die Funktionalgleichung die Werte im Konvergenzbereich die in seinem Spiegelbild, einer linken Halbebene, festlegen (allerdings nicht die im „kritischen“ Streifen, wie $s = 1$ im Falle der Hasse-Weil-L-Funktion). Schon wenn man vom Residuum einer Dedekindschen Zetafunktion an der Stelle $s = 1$ nur reden will (eine Größe, welche die wichtigsten numerischen Invarianten des Körpers in sich vereint), muß man die Funktion schon (wenigstens für ein ε) über die Achse $\mathrm{Re}\, s = 1$ nach links fortgesetzt haben. Demnach ist es der „unterirdische“ Prozeß der analytischen Fortsetzung, der die in den Zetafunktionen steckenden Informationen eigentlich freisetzt. Das klassische Verfahren dazu, von Hecke zur Vollendung gebracht, besteht darin, die fragliche Funktion (zunächst in ihrem ursprünglichen Existenzbereich) als eine Integraltransformierte einer automorphen Funktion darzustellen. Dem Integral sieht man die Fortsetzbarkeit unmittelbar an, und die Automorphie des Integranden sorgt für die Funktionalgleichung; siehe **[Bu]**, 1.1 für eine besonders durchsichtige Darstellung dieses Prozesses. Tate hat in seiner Dissertation einen grundsätzlich andern Weg eröffnet. Er schreibt die Gamma- wie die Eulerfaktoren als lokale Integrale von einem Standardtyp (so daß die Gammafaktoren als Eulerfaktoren im Unendlichen erscheinen) und beweist für sie lokale Funktionalgleichungen, die dann global zusammengesetzt werden. Wesentliche Hilfsmittel sind, wie im klassischen Verfahren, Fourieranalysis und Poissonformel, aber nicht mehr nur im Reellen bzw. Komplexen, sondern auch im p-Adischen. Man kann, wenn auch mit großer Vereinfachung, sagen, daß damit nicht nur für die Funktionalgleichung, sondern auch ihren Beweis ein Lokal-Global-Prinzip aufgewiesen ist; und damit werden die gewaltigen Verallgemeinerungen im Programm von Langlands erst möglich.

12

Aus diesem Programm, das sich mittlerweile zu einem mathematischen Kosmos entwickelt hat, können wir hier, unserm Thema gemäß, nur einen kleinen, allerdings zentralen Ausschnitt zur Sprache bringen [1]. Zunächst haben wir zu überlegen, welche Objekte hier als globale anzusehen sind. Bei Varietäten X ergibt sich die Einteilung in globale, lokale und adelische von selbst, $X(K)$, $X(K_v)$ und $X(\mathbf{A}(K))$; hinzu kommen arithmetische Objekte $X(O_K)$ und „Objekte im kleinsten“, die durch Reduktion von X modulo der Primideale von O_K entstehen und die man den lokalen zuordnen kann. Im Langlandsprogramm geht es primär um Darstellungen. Als „globale Darstellungen“ wird man in der Zahlentheorie die Darstellungen globaler Galoisgruppen ansehen. Ihnen entsprechen gemäß der (vermuteten) Langlands-Korrespondenz automorphe Darstellungen einer Gruppe GL_n über einem Zahlkörper. Als die „globalen Objekte“ der Langlandstheorie nehmen wir demnach die *automorphen Darstellungen* reduktiver (linear) algebraischer Gruppen G über globalen Körpern K; das sind (gewisse) Darstellungen π der adelischen Gruppe $G(\mathbf{A}(K))$ (die adelischen Objekte der Theorie). Solche sind im allgemeinen Tensorprodukte von Darstellungen π_v der lokalen Gruppen $G(K_v)$ (die lokalen Objekte); dabei sind diese, entsprechend der Restriktion im

1 Für allgemeine Einführungen in das Programm, aus denen alles hier Referierte geschöpft ist, siehe **[Ge]** und den Band **[BG]**; auch den Beitrag von Cogdell in **[CKM]**.

Adelbegriff, einer Restriktionsbedingung unterworfen: fast alle sind „unverzweigt“; darüber hinaus tritt bei der Bildung der Tensorprodukte eine Komplikation auf, da ein unendliches Produkt von Hilberträumen kein solcher mehr ist, sondern noch komplettiert werden muß [1]. Da die lokalen Gruppen und damit auch die adelische Gruppe Haarsche Maße tragen, können wir von L_2-Funktionenräumen sprechen. Die automorphen Darstellungen von G über K sind nun definitionsgemäß Teildarstellungen von $L_2(G(\mathbf{A}(K))/G(K))$, also Räume von Funktionen auf der adelischen Gruppe, die invariant unter der Operation der diskreten Untergruppe G(K) sind. Wir erkennen sofort den Unterschied zu unsern früheren Beispielen: während bei diesen die lokalen Objekte aus den globalen abgeleitet waren, werden hier globale Objekte *definiert* als Aggregate aus lokalen, die einer „Geschlossenheitsbedingung“ genügen, eben der G(K)-Invarianz. Die lokalen Objekte π_v sind gut verstanden; das Syntheseproblem spielt also hier a limine eine dominierende Rolle, wie jetzt erklärt werden soll, wobei wir uns auf (aller-)einfachste Termini beschränken müssen. Der K-Gruppe G (die hier ja genaugenommen als *Gruppenfunktor* {kommutative K-Algebren} → {Gruppen} auftritt) wird eine komplexanalytische Gruppe ${}^LG^0$ zugeordnet, z.B. für $G = GL_n$ ist ${}^LG^0 = GL_n(\mathbb{C})$. Ihre entscheidende Eigenschaft ist, daß (irreduzible) unverzweigte Darstellungen π_v von $G(K_v)$ durch Konjugationsklassen $t(\pi_v)$ von ${}^LG^0$ parametrisiert werden (für alle endlichen v!). Zum vollen *Langlands-Dual* ${}^LG$ muß man ${}^LG^0$ mit einer Galoisgruppe über K zu einem semidirekten Produkt verknüpfen. Im Zentrum des gesamten Programms steht nun die bisher nur in Spezialfällen bewiesene Vermutung der *Funktorialität*: sind H, G reduktive K-Gruppen und ist $r: {}^LG \to {}^LH$ ein „zulässiger“ Homomorphismus, so gibt es zu jeder (irreduziblen) automorphen Darstellung $\pi = \otimes \pi_v$ von G eine automorphe Darstellung $\pi' = \otimes \pi'_v$ von H derart, daß $r(t(\pi_v)) = t(\pi'_v)$ für alle unverzweigten v ist. Offensichtlich ist dies nichts anderes als eine Instanz des Syntheseproblems.

Die Langlands-Funktorialität erscheint auf den ersten Blick vielleicht als etwas bloß Technisches: Automorphie wird erhalten unter zulässigen Homomorphismen. Dennoch ist die Tragweite dieser Aussage kaum abzuschätzen[2] . Nur ein Aspekt soll hervorgehoben werden, von besonderm Interesse für die Zahlentheorie: Es ist leicht, die Funktorialität in eine Aussage über L-Reihen zu übersetzen, wobei die L-Reihe $L(s,\pi)$ einer automorphen Darstellung $\pi = \otimes \pi_v$ an den unverzweigten v die Eulerfaktoren

$$\det (1 - t(\pi_v)\, NP^{-s})^{-1}$$

hat (P sei das v entsprechende Primideal). Nun ist bekannt (Jacquet, Langlands), daß solche L-Reihen für $G = GL_n$ „gute“ sind, d.h. (1) sie sind meromorph fortsetzbar, (2) genügen einer Funktionalgleichung, (3) sind beschränkt in senkrechten Streifen [3]; ferner holomorph, wenn π die Einsdarstellung nicht enthält. Da jede lineare Gruppe

1 Man bemerke, daß die Darstellungen der globalen Gruppen G(K) (die globalen Objekte der *Varietäten* G) in der Theorie (paradoxerweise) gar nicht vorkommen; das wäre auch eine hoffnungslose Sache.

2 Der Verfasser jedenfalls gibt ohne weiteres zu, daß er sich dafür nicht kompetent fühlt; für Näheres siehe **[Ge]**, Kap.IV, wo unter anderm gezeigt wird, daß die Langlands-Korrespondenz selbst eine formale Konsequenz der Funktorialität ist.

3 Gelegentlich findet sich dafür der Ausdruck „nice“. Da die drei Eigenschaften meistens gemeinsam auftreten, sollte man ein Wort dafür haben. „Beschränkt in senkrechten Streifen“ bedeutet: beschränkt für $\mathrm{Im}\, s \to \pm\infty$; das schließt einen Pol im Endlichen nicht aus.

Einbettungen in ein GL_n besitzt, folgt aus der Funktorialität, daß alle automorphen L-Reihen „gut“ sind. Eine lineare Darstellung einer Galoisgruppe ist ein zulässiger Homomorphismus, und ihre L-Reihe ist die von Artin eingeführte; daraus folgt die Artinsche Vermutung, daß solche Funktionen holomorph sind, wenn die Darstellung nicht die triviale enthält. Sehr viel allgemeiner wird erwartet, daß motivische L-Funktionen automorph sind, also „gut“ (Milne nannte das die „big modularity conjecture“, **[Mi]**, S.15).

Kriterien dafür, wann eine Familie lokaler π_v ein automorphes π konstituiert, laufen heute unter dem Namen „converse theorems“. Die ersten Resultate stammen aus einer Zeit, da man die automorphen Funktionen noch nicht unter dem Gesichtspunkt adelischer Darstellungen studierte. Der Übergang von jenen zu diesen sei nur skizziert: eine klassische Modulform f ist eine Funktion auf der oberen Halbebene, diese ein homogener Raum von $SL_2(\mathbb{R})$; man kann also f zunächst zu einer Funktion auf $SL_2(\mathbb{R})$ hochheben, sodann mittels der starken Approximation für SL_2 auf die adelische Gruppe $SL_2(\mathbf{A}(\mathbb{Q}))$ ausdehnen; die Automorphiebedingung von f sorgt dann für die Invarianz der so erhaltenen Funktion unter der Operation von $SL_2(\mathbb{Q})$. Diese Funktion gehört zum regulären $SL_2(\mathbf{A}(\mathbb{Q}))$ – Modul, erzeugt damit also eine automorphe Darstellung dieser Gruppe[1] . Ein frühes *converse theorem* im Rahmen der klassischen Theorie stammt von Hecke; er bewies ein Kriterium dafür, wann eine Dirichletreihe von einer Modulform für $SL_2(\mathbb{Z})$ herstammt, explizit: wann die Koeffzienten a_n einer Dirichletschen Reihe $\Sigma a_n n^{-s}$ gleichzeitig die einer Modulform (für die volle Modulgruppe) in q-Entwicklung sind. Weil bewies eine Verallgemeinerung, die auch Modulformen für Kongruenzuntergruppen von $SL_2(\mathbb{Z})$ einbezieht; in das Kriterium gehen jetzt „getwistete“ Reihen mit Koeffizienten $a_n\ \chi(n)$ ein [2], für „genügend viele“ Dirichlet-charaktere χ . Die stärksten modernen Resultate stammen von Cogdell und Piatetski-Shapiro und können als (sehr weit gehende) Verallgemeinerungen des Weilschen angesehen werden.

13

Hier beenden wir unsern Rundgang. Daß wir keineswegs alle Aspekte der Lokal-Global-Beziehungen berührt haben, wird deutlich, wenn man sich nach arithmetischen Problemen umsieht, in denen lokale Methoden *keine* Rolle spielen. Bei den linearen Gruppen G scheinen dies alle spezifischen Probleme der diskreten Gruppen $G(\mathbb{Z})$ zu sein, wie die Frage nach Erzeugern und Relationen oder das Wortproblem, denn die lokalen Analoga $G(\mathbb{Z}_p)$ sind nicht diskret, sondern „im Gegenteil“ kompakt (oft *maximal* kompakt in der p-adischen Liegruppe $G(\mathbb{Q}_p)$), so daß jene Fragen gar keinen Sinn haben. Aber wir haben bei der Besprechung der Tamagawazahl gesehen, daß die p-adischen Gruppen dennoch in gewissem Sinne „hereinspielen“; sichtbarer wird das bei der Behandlung des Kongruenzproblems [3]. Die Klassenzahlen der Zahlkörper *haben* lokale Analoga, nur sind diese alle trivial[4]; dennoch kann man ganz andere lokale Objekte,

1 Details z.B. in dem Aufsatz von Kudla, in **[BG]**, S.133ff.

2 Siehe **[Bu]**, 1.5.

3 Das ist die Frage, ob jede Untergruppe von endlichem Index eine Kongruenzgruppe enthält; siehe **[BMS]**. In die Definition des „Kongruenzkerns“, der die Abweichung davon „mißt“, geht das adelische Objekt ein.

4 Leider, muß man fast sagen; denn wären sie es nicht, und wären die globalen durch sie auch nur teilweise

nämlich p-adische L-Funktionen zu Aussagen über Klassenzahlen heranziehen [1]. Lokale Methoden scheinen a priori wirkungslos, wo es um Beziehungen zwischen verschiedenen Primzahlen geht. Aber Quadratische Reziprozität ist doch wohl eine solche? Nun braucht man keine lokalen Methoden, um sie zu beweisen, aber lokale Zahlentheorie befindet sich hier doch in unmittelbarer Nachbarschaft (man denke das das Zerlegungsgesetz für quadratische Körper). Kaum vorstellen kann man sich freilich, daß lokale Methoden bei Fragen der Primzahlverteilung oder der additiven Zahlentheorie (wie dem Euler-Goldbach-Problem) hilfreich werden. Aber wer will hier ein abschließendes Urteil wagen?

Diese Beispiele lehren, daß sich die Lokal-Global-Beziehungen nicht ohne weiteres klassifizieren lassen, jedenfalls nicht durch die einfache Liste, die wir in Abschnitt 3 zum Ausgangspunkt genommen haben. Eher könnte man vermuten, daß es soviele Arten solcher Beziehungen gibt wie arithmetische Probleme überhaupt. Die Liste suggerierte auch, daß die Komplettierungen der Zahlkörper eine bloß dienende Funktion haben. Für den Zahlentheoretiker, dem die arithmetischen Objekte die Hauptsache sind, mag eine solche Auffassung eine unvermeidbare *deformation professionelle* sein. Aber vom Ganzen aus gesehen ist der Begründungszusammenhang mit allen seinen Instanzen das, worauf es ankommt. Daß übrigens eine solche Auffassung von der archimedischen Komplettierung von $\mathbb{Q}$ der größte Unsinn wäre, bedarf keiner Ausführung; aber auch die p-adischen Körper sind mittlerweile in der Physik angekommen **[RTV]**. Vielmehr sollte man das Lokale in seiner Gesamtheit, unendlich viele kontinuierliche, vollständige, paarweise inkompatible, nur durch den gemeinsamen Primkörper verbundene Welten, als eine Art Grundgeflecht oder Myzel für die diskreten globalen Objekte betrachten, die wie Kristalle darin eingebettet sind. Ihr *principium individuationis* zu verstehen, ist die große Aufgabe.

Literatur

[A] E.Artin, Algebraic Numbers and Functions, London 1968

[AM] M.Atiyah / I.G.Macdonald, Introduction to Commutative Algebra, Addison-Wesley 1969

[AT] E.Artin / J.T.Tate, Class Field Theory, Reading 1967

[B] N.Bourbaki, Commutative Algebra, Paris 1972

[BMS] H.Bass / J.Milnor / J.-P.Serre, Solution of the Congruence Subgroup Problem... Publ.I.H.E.S. 33 (1967) 59-137 (= Serre Oeuvres II, Nr.74).

bestimmt, so wüßten wir wahrscheinlich mehr über die letzteren, z.B. ob sie unendlich oft = 1 sind.
1 Siehe **[Wa]** Ch.7. In diesem Fall sind die lokalen Objekte übrigens ebenso komplex wie ihre globalen Urbilder.

[BG] J.Bernstein / S.Gelbart (edts), An Introduction to the Langlands Program, Birkhäuser 2003

[BS] A.Borel / J.-P.Serre, Théorèmes de finitude en cohomologie galoisienne, Comm.Math.Helv. 39 (1964) 111-164

[Bu] D.Bump, Automorphic Forms and Representations, Cambridge UP 1998

[CF] J.W.S.Cassels, A.Fröhlich (edts), Algebraic Number Theory, Academic Press 1967

[CM] D.Coray / C.Manoil, On Large Picard Groups...., Acta Arithm.LXXVI (2) 1996

[CKM] J.Cogdell / H.Kim / M. Ram Murty, Lectures on Automorphic L-Functions, AMS 2004

[D] J.Dieudonné, A Panorama of Pure Mathematics, Academic Press 1982

[G] F.Gounelas, The Brauer-Manin Obstruction, www

[Ge] S.Gelbart, An Elementary Introduction to the Langlands Program, Bull.AMS 10 (2), 1984, 177-219

[H] H.Hasse, Zahlbericht II, Jahresber. DMV 36 (1927), 233-311

[HH] H.Hasse, History of Class Field Theory, in **[CF]**

[Ha] D.Harari, Weak Approximation on Algebraic Varieties, in **[PT]**

[J] G.Janusz, Algebraic Number Fields, Academic Press 1973

[K] E.Kleinert, Über Addition und Multiplikation, in: E.K., Studien zur Struktur der Mathematik, Leipziger Universitätsverlag 2012

[Kl] N.Klingen, Arithmetic Singularities, Oxford UP 1998

[Kn] M.Kneser, Semi-Simple Algebraic Groups, in **[CF]**

[Ko] H.Koch, Zahlentheorie, Vieweg 1997

[L] S.Lang, Algebraic Number Theory, GTM 110, Springer 1986

[La] T.Y.Lam, The Algebraic Theory of Quadratic Forms, Reading 1973

[M] B.Mazur, On the Passage from Local to Global in Number Theory, Bulletin AMS 29 (1),1993, 14-50

[MR] B.Mazur, The Topology of Rational Points, Exp.Math.1 (1992) No.1

[Ma] D.Marcus, Number Fields, Springer 1977

[Mi] J.Milne, Motives – Grothendiecks Dream, www (2009)

[N] J.Neukirch, Algebraische Zahlentheorie, Springer 1992

[OM] O.T.O'Meara, Introduction to Quadratic Forms, Springer 1973

[PRS] C.Popescu / K.Rubin / A.Silverberg (edts), Arithmetic of L-Functions, AMS 2011

[PR] V.Platonov / A.Rapinchuk, Algebraic Groups and Number Theory, Academic Press 1994

[PT] B.Poonen, Y.Tschinkel (edts), Arithmetic of Higher-Dimensional Algebraic Varieties, Birkhäuser 2004

[R] I.Reiner, Maximal Orders, Academic Press 1975

[Ro] D.E.Rohrlich, Root Numbers, in **[PRS]**

[RTV] R.Rammal/G.Toulouse/M.Virasoro, Ultrametricity for Physicists, Rev.Mod.Phys. 58 (1986) 765

[SC] J.-P.Serre, Cohomologie Galoisienne, SLN 5, Springer 1994[5]

[SG] J.-P.Serre, Topics in Galois Theory, Jones and Bartlett 1992

[Si] J.H.Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer 1985

[SW] P.Swinnerton-Dyer, Diophantine Equations: Progress and Problems, in **[PT]**

[T] J.T.Tate, Fourier Analysis in Number Fields and Heckes L-Functions, in **[CF]**

[W] A.Weil, Basic Number Theory, Springer 1974[3]

[Wa] L.Washington, Introduction to Cyclotomic Fields, Springer 1982