Nicht-Torsion in abelschen Varietäten

Peter Müller

22. Juli 2004

Proposition 0.1. *Sei K ein algebraisch abgeschlossener Körper, der nicht algebraisch ist über einem endlichen Körper. Sei A eine abelsche Varietät über K. Dann enthält $A(K)$ Elemente unendlicher Ordnung.*

Der Beweis zerfällt in mehrere Teile.

Lemma 0.2. *Für alle $n \in \mathbb{N}$ gibt es eine endlich erzeugte Erweiterung E von $\mathbb{F}_p$ mit folgenden Eigenschaften:*

(a) A ist zusammen mit den Gruppenoperationen über E definiert.

(b) Es gibt eine Galoiserweiterung L/E mit $L \subseteq K$ und $\mathrm{Gal}(L/E) = \mathrm{Alt}_n$.

Beweis. Sei F zunächst endlich erzeugt, aber nicht algebraisch über einem endlichen Körper, so dass (a) erfüllt ist. Seien $X, T_1, \ldots, T_n$ Variablen über F. Das generische Polynom $X^n + T_1X^{n-1} + \cdots + T_n$ hat Galoisgruppe Sym_n über $F(T_1, \ldots, T_n)$. Da F Hilbertsch ist ([FJ86, Theorem 12.10]), gibt es eine Galoiserweiterung L/F mit $\mathrm{Gal}(L/F) = \mathrm{Sym}_n$ und $L \subseteq K$. Sei E der Fixkörper von Alt_n in L. □

Lemma 0.3. *Es gelte die Situation im obigen Lemma. Ferner bestehe $A(K)$ nur aus Torsionspunkten. Dann gibt es $k \in \mathbb{N}$ und eine Galoiserweiterung M/E mit $E \subseteq L \subseteq M \subseteq K$ und $\mathrm{Gal}(M/E) \leq \mathrm{GL}_m(\mathbb{Z}/k\mathbb{Z})$ mit $m = 2\dim A$.*

Beweis. Offenbar gilt $K = E(A(K))$. (Man projiziere von einem affinen Teil von A auf eine nicht-konstante Koordinate.) Aber $E(A(K))$ wird über E von den Koordinaten von $A_u(K)$ ($u \in \mathbb{N}$) erzeugt. (A_u ist u-Torsion.) Es gibt also eine endliche Teilmenge $U \subset \mathbb{N}$, so dass $L \subseteq E(A_u(K), u \in U)$. Sei nun k das kleinste gemeinsame Vielfache der $u \in U$. Es folgt $L \subseteq E(A_k(K)) = M'$. Nun operiert $\mathrm{Aut}(M'/E)$ treu auf der k-Torsion. Sei M der separable Abschluss von E in M'. Dann gilt $L \subseteq M$ (da L separabel über E ist). Ferner ist M'/M rein inseparabel, die Einschränkung von $\mathrm{Aut}(M'/E)$ auf die Galoiserweiterung M von E ist daher treu. Es folgt $\mathrm{Gal}(M/E) \leq \mathrm{GL}_m(\mathbb{Z}/k\mathbb{Z})$. $\square$

Aus den Lemmata folgt nun sofort via Galoiskorrespondenz

Lemma 0.4. *Die Behauptung der Proposition sei falsch. Dann gibt es für alle $n \geq 5$ ein $k \in \mathbb{N}$, so dass $\mathrm{GL}_m(\mathbb{Z}/k\mathbb{Z})$ eine Untergruppe G enthält, so dass Alt_n ein Quotient von G ist.*

Zunächst betrachten wir eine Reduktion von k auf den Fall einer Primpotenz und dann auf eine Primzahl. Bei vorgegebenen n und k nehmen wir mal an, G sei mit $|G|$ minimal gewählt. Sei $N \triangleleft G$ mit $G/N = \mathrm{Alt}_n$. Für p ein Primteiler von k sei p^e die höchste Potenz, die k teilt. Sei $\mathrm{GL}_m(\mathbb{Z}/k\mathbb{Z}) \to \mathrm{GL}_m(\mathbb{Z}/p^e\mathbb{Z})$ die natürliche Surjektion, und N_p der Kern. Wegen der Einfachheit von G/N gilt entweder $N_p \leq N$, oder $NN_p = G$. Im ersten Fall können wir also k durch p^e ersetzen. Falls dieser Fall nie auftritt, dann gilt $NN_p = G$ für alle Primteiler p von k. Wegen der Minimalität von G gilt stets $G = N_p$, offenbar ein Widerspruch, da die N_p sich trivial schneiden.

Daher können wir k durch p^e ersetzen. Der Kern der natürlichen Surjektion $GL_m(\mathbb{Z}/p^e\mathbb{Z}) \to \mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ ist eine p-Gruppe. Die Alt_n überlebt also diese Surjektion, und wir dürfen sogar $k = p$ annehmen.

Die folgende Proposition beweist die ursprüngliche Behauptung.

Proposition 0.5. *Für alle $m \in \mathbb{N}$ gibt es eine Konstante C_m mit folgender Eigenschaft: Ist Alt_n Quotient einer Untergruppe von $\mathrm{GL}_m(p)$ für eine Primzahl p, dann gilt $n \leq C_m$.*

Beweis. Sei m minimal, so dass die Aussage falsch ist. Sei $G \leq \mathrm{GL}_m(p)$, $N \triangleleft G$ mit $G/N = \mathrm{Alt}_n$. Wieder sei (bei festem n) $|G|$ minimal. Dann gilt $HN < G$ für alle maximalen Untergruppen H von G, also $N \leq H$. Daher liegt N in der Frattini-Gruppe von G, und ist somit nilpotent. Aus $G \leq \mathrm{GL}_m(p)$ folgt die triviale Abschätzung $n!/2 \leq p^{m^2}$. Für große n gilt daher $p > n$, insbesondere ist G/N eine p'-Gruppe. Wir unterscheiden zwei Fälle:

(i) N ist auch eine p'-Gruppe. Dann ist G eine p'-Gruppe, und wir können nach Charakteristik 0 liften, also $G \leq \mathrm{GL}_m(\mathbb{C})$ ([Hup67, Hauptsatz 12.9]). Ein klassischer Satz von Jordan [Isa76, Theorem 14.12] besagt nun, dass es eine nur von m abhängige Konstante D_m gibt, so dass in unserer Situation

G einen abelschen Normalteiler B mit $|G/B| \leq D_m$ hat. Insbesondere gilt $n!/2 \leq D_m$, und wir sind fertig.

(ii) Nun habe N eine nicht-triviale p-Sylowgruppe P. Wegen der Nilpotenz von N ist P normal in G. Da G/N eine p'-Gruppe ist hat P ein Komplement C in G (Schur-Zassenhaus). Aber $C/(C \cap N) = \mathrm{Alt}_n$, im Widerspruch zur Minimalität von $|G|$. □

Mittels des Larsen-Pink Analogons obigen Satzes von Jordan in Charakteristik p erhält man folgende Verschärfung:

Proposition 0.6. *Für alle $m \in \mathbb{N}$ gibt es eine Konstante C_m mit folgender Eigenschaft: Sei S eine einfache nicht-abelsche Gruppe der Ordnung $> C_m$. Ferner gelte: Ist S eine Gruppe vom Lietyp in Charakteristik r, dann gilt $|S| \geq r^{m^2}$. Dann gibt es für keine Primzahl p eine Untergruppe $G \leq \mathrm{GL}_m(p)$, so dass S ein homomorphes Bild von G ist.*

Beweis. Sei wieder $|G|$ minimal mit $G/N = S$. Wie im alternierenden Fall folgt, dass N nilpotent. Nach [LP, Theorem 0.2] hat G Normalteiler $G_2 \leq G_1$ mit folgenden Eigenschaften:

(a) $|G/G_1| \leq C_m$, wobei C_m eine nur von m abhängige Konstante ist.

(b) $G_1 = G_2$, oder G_1/G_2 ist direktes Produkt einfacher Gruppen vom Lietyp in Charakteristik p.

(c) G_2 ist auflösbar. ([LP] gibt eine genauere Beschreibung von G_2.)

In unserem Fall kann $G_1 = G_2$ nicht gelten, denn es folgte $G_2 \leq N$, also $|S| \leq |G/G_2| = |G/G_1| \leq C_m$. Daher gilt $G_1/G_2 = S$. Aber $G_1 \leq \mathrm{GL}_m(p)$, also $|S| \leq |G_1| \leq p^{m^2}$. □

Literatur

[FJ86] M. Fried, M. Jarden, *Field Arithmetic*, Springer–Verlag, Berlin Heidelberg (1986).

[Hup67] B. Huppert, *Endliche Gruppen I*, Springer–Verlag, Berlin Heidelberg (1967).

[Isa76] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York (1976), Pure and Applied Mathematics, No. 69.

[LP] M. J. Larsen, R. Pink, *Finite subgroups of algebraic groups*, Preprint 1998, available from http://www.math.ethz.ch/˜pink/.