Pacific Journal of Mathematics

BRAUER-TYPE RESULTS ON SEMIGROUPS OVER p-ADIC FIELDS

Janez Bernik

Volume 208 No. 2 February 2003

PACIFIC JOURNAL OF MATHEMATICS
Vol. 208, No. 2, 2003

BRAUER-TYPE RESULTS ON SEMIGROUPS OVER p-ADIC FIELDS

Janez Bernik

In this paper we show that every central simple algebra A over $\mathbb{Q}_p$, generated by a multiplicative semigroup $S \subset A$ with the property that the minimal polynomial of every element in S splits over $\mathbb{Q}_p$, is isomorphic to $M_n(\mathbb{Q}_p)$. If, in addition, $S \subset A^*$ is a compact group, then it contains a commutative normal subgroup of finite index.

1. Introduction.

In this paper we consider the following problem. Let $k < K$ be fields. Suppose $S \subset M_n(K)$ is an absolutely irreducible multiplicative semigroup with the property that the spectrum of every $a \in S$ is contained in k. Does it follow that S is simultaneously realizable in $M_n(k)$, that is, does there exist a $p \in GL_n(K)$ such that $pSp^{-1} \subset M_n(k)$? The overfield K plays no essential role in this situation. Consider the k-algebra A generated by S. It is easy to see that it is a central simple algebra over k (see [**7**]). If one can show that A is isomorphic to $M_n(k)$, then this isomorphism can be extended to an inner isomorphism of $M_n(K)$ by Skolem-Noether theorem. So we consider the more intrinsic version of the question above. Suppose A is a central simple algebra over k and $S \subset A$ a multiplicative semigroup that generates A as a k-vector space and has the property that the minimal polynomial of every element in S splits over k. Does it follow $A \simeq M_n(k)$? If we exclude the case when the Brauer group of k is trivial, then the question has no apparent answer. If S is a finite subgroup of A^* and $\mathrm{char}\,(k) = 0$, then the answer is affirmative by Brauer's theorem on splitting fields (see [**3**, Thm. 41.1]).

The general semigroup case was considered for some particular fields. In [**7**] it is shown that the answer is affirmative in the special case $k = \mathbb{R}$ with no additional assumptions on S (see also [**9**] for some related results). In this paper we consider the case $k = \mathbb{Q}_p$ for every rational prime number p.

The proof proceeds in two steps. First we consider the special case when S is a compact subgroup of A^*. The crucial part in this case is the fact that the Lie algebra of S is commutative. This however is not true if k is a general p-adic field (see the example at the end of the paper). The second step is to reduce the problem from arbitrary semigroup with the desired property to

the compact group case. Although we state this result for $k = \mathbb{Q}_p$ only, the reader can easily verify that this reduction works for any p-adic field.

2. The results.

We start with a simple observation that holds true for any field k. Let $\mu_n(k)$ denote the group of n-th roots of unity in k.

Proposition 1. *Let A be a central simple algebra over a field k. Suppose A is spanned over k by a center-by-finite group $S \subset A^*$ with the property that the minimal polynomial of every $s \in S$ splits over k. Then $A \simeq M_n(k)$.*

Proof. We assume with no loss of generality that $k^* < S$ and let r denote the exponent of the finite group S/k^*. The conditions of the proposition imply that every element $a \in S$ is a scalar multiple of an element $b \in S$ where $b^r = 1$. Now, let $a, b \in S$ be two elements of order dividing r. Their product $c = ab$ may be of order greater than r but $c = \alpha d$, $\alpha \in k^*$, $d \in S$, $d^r = 1$. Applying the reduced norm we see that

$$\alpha^{nr} = \mathrm{nr}(c^r) = \mathrm{nr}((ab)^r) = \mathrm{nr}(a^r)\mathrm{nr}(b^r) = 1$$

where n is the reduced degree of A over k. Thus we have shown that

$$S_1 = \{\alpha b; \alpha \in \mu_{nr}(k), b \in S, b^r = 1\}$$

is a subgroup of S of bounded period which clearly spans A. By a well-known result by Burnside this implies S_1 is finite (the reduced trace on A is nondegenerate and it takes only finitely many values on S_1).

Suppose now $\mathrm{char}\,(k) = 0$. If m is the exponent of S_1, then it is easy to see that k contains a primitive m-th root of unity so we can apply the Brauer's theorem on splitting fields and the proof is complete in this case. If $\mathrm{char}\,(k) \neq 0$, then the claim follows from ([**4**], Proof of Corollary 7.11, p. 148).

It should be mentioned that there is an alternative but less elementary way to prove this result by using Schur's theory of projective representations of finite groups. Observe also that in the particular case when $\mathrm{char}\,(k) = 0$ and the only roots of unity in k are ± 1 (e.g., $k = \mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3$) S_1 is of exponent 2, therefore commutative and $A \simeq k$.

In what follows we will need a slight generalization of the previous proposition. We shall also use repeatedly the following fact. If one wants to show the triviality of a central simple algebra A in the Brauer group of k, then it suffices to consider the central simple algebra eAe where $e \in A$ ia a nonzero idempotent. The proof may be found in [**5**].

Corollary 2. *Let A be a central simple algebra over a field k. Suppose A is spanned over k by a group $S \subset A^*$ which contains an abelian subgroup of finite index and has the property that the minimal polynomial of every $s \in S$ splits over k. Then $A \simeq M_n(k)$.*

Proof. Let S_1 denote the abelian subgroup of finite index in S. Observe that S_1 has a subgroup that is both normal and of finite index in S (the kernel of the action of S on the set of left cosets S/S_1) so there is no harm in assuming that S_1 is normal in S. Let B be the k-algebra generated by S_1. By Clifford's theorem (see [**3**]) B is semisimple and since it is commutative it is isomorphic to a direct sum of m copies of k for some m. Let $\{e_1, \dots, e_m\}$ be the set of minimal orthogonal idempotents in B upon which S acts transitively by conjugation and set $C = C_S(e_1)$ the centralizer of e_1 in S. It is clear that given $a \in S$ we have $e_1 a e_1 \neq 0$ precisely when $a \in C$. So the central simple algebra $e_1 A e_1$ is spanned by a center-by-finite group Ce_1 (a homomorphic image of C) which obviously has the property that the minimal polynomial of every element in Ce_1 splits over k and the claim follows by the previous proposition.

From now on we suppose, unless stated otherwise, that $k = \mathbb{Q}_p$, i.e., k is a non-archimedian locally compact field that contains $\mathbb{Q}$ as a dense subfield. We fix an absolute value $|\cdot|$ on k and let o_k denote the ring of p-adic integers. For most of the facts concerning algebraic groups we refer the reader to [**2**].

Theorem 3. *Let A be a central simple algebra over k. Suppose A is spanned over k by a compact group $S \subset A^*$ with the property that the minimal polynomial of every element in S splits over k. Then $A \simeq M_n(k)$ and S contains a commutative normal subgroup of finite index.*

Proof. Let G be the Zariski closure of S in $\underline{A}^*$. Then G is an algebraic group defined over k. The absolute irreducibility of S clearly implies that the connected component of the unit G^0, if not trivial, is a reductive group defined over k. If G^0 is trivial, then S is a finite group and the theorem follows, therefore we assume that G^0 is not trivial. Being reductive, it is an almost direct product of its central torus T and a semisimple group $H = (G^0, G^0)$ where both T and H are defined over k.

We want to show that H is trivial so we assume the contrary. Now the group $S_1 = S \cap G^0$ is also compact, therefore it is a Lie group over k by Cartan's theorem (see [**12**]). Its Zariski closure is precisely G^0. We know, that the Zariski closure of (S_1, S_1) is H and consequently it is the Zariski closure of $S_2 = S \cap H$. This latter group is also compact and we let $L_a(S_2)$ denote its Lie algebra in the sense of [**12**]. By [**8**, Prop. 3.4] $L_a(S_2)$ is a Lie ideal in $L_a(H(k)) = L(H)(k)$. But this is a semisimple Lie algebra which, together with Zariski density and compactness of S_2, implies $L_a(S_2) = L(H)(k)$. To see this assume $L(H)(k) = L_a(S_2) \oplus V$ where $V \neq 0$ is the unique ideal in $L(H)(k)$, complementary to $L_a(S_2)$. Consider the restriction to V of the adjoint representation of $H(k)$. The conditions imply that S_2 is mapped to a discrete compact group, therefore finite, but on the other hand Zariski dense in a nontrivial semisimple group, a contradiction.

Since $L_a(S_2) = L(H)(k)$ the group S_2 contains a subgroup that is open in $H(k)$. But every semisimple group H over a p-adic field k contains a maximal k-torus that is anisotropic over k (see [**8**, Thm. 6.21]) and it follows that there are elements arbitrarily close to identity in $H(k)$ that cannot be diagonalized over k and again we have a contradiction. Therefore H is trivial and subsequently S_1 is an abelian normal subgroup of finite index in S and the claim follows by Corollary 2.

Remark 4. If the field k in the previous theorem were a general p-adic field one could still infer that S_2 is a Lie group over $\mathbb{Q}_p$, $\mathbb{Q}_p < k$. But in this case its Lie algebra $L_a(S_2)$, which need not be trivial (see the example at the end of the paper), is just a $\mathbb{Q}_p$-subalgebra in $L(H)(k)$. In fact the same argument as above shows that it is never a nontrivial ideal in $L(H)(k)$.

Keeping the notation of the previous theorem we also have the following corollary.

Corollary 5. *The exponent of the finite group S/S_1 divides the number of roots of unity in k and the same is true for G/G^0.*

Proof. The statement is obvious if S_1 is trivial so we assume the contrary. Let m denote the number of roots of unity in k. Now the first assertion follows by observing that given $a \in S$ the power a^m belongs to domain of convergence of the log series. Therefore we have $a^m = \exp(b)$, $b \in L_a(S) = L_a(S_1)$ and $a^m \in S_1$ by the definition of S_1. The second assertion follows immediately from Zariski density of S in G.

Theorem 6. *Let A be a central simple algebra over k. Suppose A is spanned over k by a multiplicative semigroup $S \subset A$ with the property that the minimal polynomial of every element in S splits over k. Then A is isomorphic to $M_n(k)$.*

Proof. Observe that we can view A as matrices over some finite complete extension K of k . The semigroup S is then an absolutely irreducible matrix semigroup in $M_n(K)$ with the property that the spectrum of every $a \in S$ is contained in k. This property is preserved under multiplication by scalars in k, but also under norm closure, which follows from the continuity of spectrum, a consequence of Krasner's Lemma (see [**6**]). So we may assume that S is a closed subset of A (and $M_n(K)$) and $S = kS = \{\lambda s; \lambda \in k, a \in S\}$. Now let r be the minimum of the ranks of the nonzero elements in S. We claim that there is a rank r element $a \in S$ that is not a nilpotent. Assume the contrary. Let $b \in S$ have rank r. Then the semigroup SbS is a semigroup of nilpotents and by Levitzky's theorem (see also [**1**]) it generates a nontrivial nilpotent ideal in A but A is simple, hence the contradiction. Next we claim that there is an idempotent $e \in S$ with rank r. Let $a \in S$ be a nonnilpotent element of this minimal rank. By dividing it with an appropriate element

of k^* we may assume that all the eigenvalues lie in the unit ball and that some (say m) have absolute value 1. By replacing a with some power of it we may further assume that all the eigenvalues with absolute value 1 belong to $1 + po_k$, where p is the characteristic of the residue class field. Let $a = a_s + a_n$ be the Jordan decomposition of a with $a_n^k = 0$ for some k. Consider the sequence

$$a^{p^n} = \sum_{j=0}^{k-1} \binom{p^n}{j} a_s^{p^n - j} a_n^j$$

for n large enough. It is easy to see that this sequence converges to an idempotent $e \in S$ of rank m, so $m = r$ by minimality of rank. Consider the semigroup eSe. It clearly satisfies the conditions of S and it generates the central simple k-algebra eAe. The theorem will be proved provided we show $eAe \simeq M_r(k)$.

Replacing eAe for A we see that one can assume that $S \subset A$ is a closed semigroup in which every nonzero element is invertible and all the eigenvalues of an element in S have equal absolute value. Consider the set $S_1 = \{a \in S; |nr(a)| = 1\}$ which is clearly also a closed semigroup in A. Observe that $a \in S$ belongs to S_1 precisely when all its eigenvalues lie in o_k^* and so every element of S_1 is integral over o_k. Since S_1 generates A as a vector space over k we have to show that S_1 is a compact group and then apply the previous theorem.

Consider the o_k algebra $\Gamma \subseteq A$, generated by S_1. Then by [**1**] every element of Γ is integral over o_k. By [**10**, Thm. 10.3] Γ is an o_k-order in A and therefore contained in a maximal o_k-order Δ. The latter is compact and so is $S_1 \subset \Delta$. The only idempotent in the compact semigroup S_1 is the identity, so by [**11**, Thm. 3.5] S_1 is a compact group and the proof is complete.

As a corollary we obtain the following result which is already implicit in [**9**].

Corollary 7. *Let A be a central simple algebra over $\mathbb{Q}$. Assume A is spanned by a multiplicative semigroup $S \subset A$ with the property that the minimal polynomial of every element in S splits over $\mathbb{Q}$. Then A is isomorphic to $M_n(\mathbb{Q})$.*

Proof. By the Hasse-Brauer-Albert-Noether theorem [**10**, Thm. 32.11] it suffices to show that $A_P = A \otimes \mathbb{Q}_P$ is trivial in the Brauer group $\mathbf{Br}(\mathbb{Q}_P)$ for every prime P. If P is finite, then $\mathbb{Q}_P = \mathbb{Q}_p$ for some rational prime p and we apply the previous theorem for the image of S under natural embedding. Since there is only one infinite prime P over $\mathbb{Q}$, namely $\mathbb{Q}_P = \mathbb{R}$, we also have that A_P is trivial in this case by the product formula.

3. Some examples and remarks.

Example 8. As our first example we take the group of matrices $S \subset M_2(k)$, generated by $S_1 = \{\mathrm{diag}\,(\alpha^2, \beta^2); \alpha, \beta \in o_k^*\}$ and t, where t is the matrix of the transposition of the standard basis of k^2. An easy computation shows that this is indeed a compact irreducible group with the desired property. This example can easily be generalized to matrices of order 2^n.

The next example shows that, although there are good reasons to believe that both the theorems of this article hold for any p-adic field k, the structure of the compact group S with the desired properties can be much more complicated in this general case.

Example 9. Let k be a p-adic field and n a fixed number. Then there exists a finite extension field $l > k$ with the property that every polynomial of degree less or equal to n in $k[X]$ splits over l (see [**8**, Prop. 6.13]). Let A be a central simple algebra of reduced degree n over k and $\Delta \subset A$ a maximal order in A. Let S be the image of Δ^* under natural embedding $A \to A \otimes_k l \simeq M_n(l)$, $a \mapsto a \otimes 1$. Clearly S is compact, it spans $M_n(l)$ and the minimal polynomial of every $s \in S$ splits over l.

We conclude with a remark and some open questions.

Remark 10. Let k be either $\mathbb{Q}_p$ or $\mathbb{R}$. It is an interesting question whether there exists an absolutely irreducible group $S \subset GL_n(k)$ such that the spectra of its elements lie in k and such that the Zariski closure of S is semisimple. A similar argument as in the proof of Theorem 3 shows that such a group is necessarily discrete and, consequently, its Zariski closure not k-anisotropic. It is known (see [**13**]) that $SL_2(k)$ contains a free Zariski dense subgroup S and one can check easily that the spectra of all its elements under any k-representation of SL_2 lie in k. It is an open question what are the necessary and sufficient conditions on a semisimple group (for instance being k-split) in order for it to be the Zariski closure of a group S with the desired property.

References

[1] S.A. Amitsur, *On the characteristic polynomial of a sum of matrices*, Linear and Multilinear Algebra, **8** (1980), 177-182, MR 82a:15014, Zbl 0429.15006.

[2] A. Borel, *Linear Algebraic Groups*, 2-nd ed., Graduate Texts in Mathematics, **126**, Springer-Verlag, New York, 1991, MR 92d:20001, Zbl 0726.20030.

[3] C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, New York, 1962, MR 26 #2519, Zbl 0131.25601.

[4] ———, *Methods of Representation Theory*, Vol. 1, Wiley, New York, 1981, MR 82i:20001, Zbl 0469.20001.

[5] P.K. Draxl, *Skew Fields*, London Mathematical Society Lecture Note Series, **81**, Cambridge University Press, Cambridge, 1983, MR 85a:16022, Zbl 0498.16015.

[6] F.Q. Gouvêa, *p-Adic Numbers*, Springer-Verlag, Berlin, 1993, MR 95b:11111, Zbl 0786.11001.

[7] M. Omladič, M. Radjabalipour and H. Radjavi, *On semigroups of matrices with traces in a subfield*, Linear Algebra Appl., **209** (1994), 419-424, MR 95e:15012, Zbl 0817.20064.

[8] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, San Diego, CA, 1994, MR 95b:11039, Zbl 0841.20046.

[9] M. Radjabalipour and H. Radjavi, *A finiteness lemma, Brauer's Theorem and other irreducibility results*, Comm. Alg., **27** (1999), 301-319, MR 99m:20152, Zbl 0920.20058.

[10] I. Reiner, *Maximal Orders*, Academic Press, London, 1975, MR 52 #13910, Zbl 0305.16001.

[11] W. Ruppert, *Compact Semitopological Semigroups: An Intrinsic Theory*, Lecture Notes in Mathematics, **1079**, Springer-Verlag, Berlin, 1984, MR 86e:22001, Zbl 0606.22001.

[12] J.-P. Serre, *Lie Algebras and Lie Groups*, Lecture Notes in Mathematics, **1500**, Springer-Verlag, Berlin, 1992, MR 93h:17001, Zbl 0742.17008.

[13] J. Winkelmann, *On discrete Zariski-dense subgroups of algebraic groups*, Math. Nachr., **186** (1997), 285-302, MR 98d:2005, Zbl 0897.14015.

Received September 9, 2001 and revised November 16, 2001.

University of Ljubljana
Faculty of Mathematics and Physics
Jadranska 19
SI-1000 Ljubljana
Slovenia
E-mail address: janez.bernik@fmf.uni-lj.si