Comptes rendus mathématiques
Mathematical Reports

26
No 3

SEPTEMBER / SEPTEMBRE 2004

IN THIS ISSUE / DANS CE NUMÉRO

65 Peter C. Gibson, Michael P. Lamoureux
Maximally symmetric, minimally redundant partitions of unity in the plane

73 Jung-Jo Lee
A remark on the ranks of twists of elliptic curves

79 W. Herfort, P. A. Zalesskii
Virtually Free Pro-p Groups

84 Erhard Neher
Lie Tori

90 Erhard Neher
Extended affine Lie algebras

C. R. Math. Rep. Acad. Sci. Canada Vol. **26**, (3), 2004 pp. 65–72

MAXIMALLY SYMMETRIC, MINIMALLY REDUNDANT PARTITIONS OF UNITY IN THE PLANE

PETER C. GIBSON AND MICHAEL P. LAMOUREUX

Presented by G. A. Elliott, FRSC

ABSTRACT. Partitions of unity that consist of translates of a single function—called the atom—over a planar lattice arise in recently developed implementations of the Gabor transform, where for numerical reasons it is desirable to maximize the symmetry of the atom. In the present article we determine the maximum symmetry that is possible for such an atom, and construct explicitly a maximally symmetric example.

RÉSUMÉ. Des partitions de l'unité qui sont composées des translations d'une seule fonction, dit l'atome, par les sommets d'un réseau dans le plan font partie des implémentations récentes de la transformée de Gabor, dont, pour des raisons numériques, il est important que l'atome soit aussi symétrique que possible. Ici on determine la symétrie maximale possible pour un tel atome, et on construit également un exemple explicite d'un atome possédant cette symétrie.

1. Introduction In recent years time-frequency analysis centred around the Gabor transform has emerged as an active area of research, with diverse applications to abstract functional analysis and to many applied areas such as imaging and signal processing. For a cross-section of papers in the subject, and for numerous references, see [1]; the text [2] provides a detailed introduction. There exist efficient numerical schemes to implement the Gabor transform that are based on partitions of unity in the plane (or more generally, in $\mathbf{R}^{2n}$), consisting of the translates over a lattice of a single function, which is referred to as the "atom" of the partition [3]. If one is using the Gabor transform to analyze data obtained from a highly structured medium, such as seismic data obtained from a horizontally layered section of the earth, it is desirable to choose a partition of unity whose atom is highly symmetrical. Otherwise there is a risk of introducing numerical artifacts that have a preferred direction, and which may obscure, or interfere with, the inherent material structure one is trying to image. This leads to a basic geometrical question which is the subject of the present article: *What is the maximum possible symmetry that the atom of a partition of unity can have?*

To begin, we make this question precise. We consider partitions of unity in the plane $\mathbf{R}^2$ of the form

$$\sum_{l \in \mathcal{L}} \alpha(x - l) \equiv 1 \qquad (x = (x_1, x_2) \in \mathbf{R}^2)\,, \tag{1}$$

Received by the editors on October 5, 2003.
AMS subject classification: 52C05.

where:

(i) $\mathcal{L}$ is a *lattice* in $\mathbf{R}^2$, i.e., a set of regularly spaced points in the plane;
(ii) $\alpha(x)$, called the *atom*, is continuous and has compact, strictly convex support;
(iii) $\alpha^{-1}(1)$ has positive measure.

The last condition guarantees that, at least on some open subset Ω of the plane, the partition (1) contains no redundancy, in that points of Ω lie in the support of a unique translate of the atom α—see Figure 1. In this sense we are considering minimally redundant partitions of unity based on a regular lattice. Henceforth we use the terms "partition" and "atom" to refer to a partition of unity in the plane and its corresponding atom, respectively, for which the above conditions (i)–(iii) are satisfied.

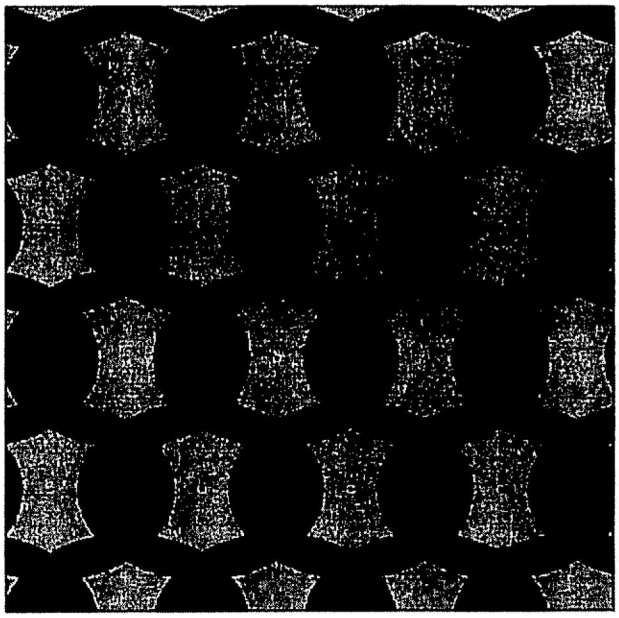

Figure 1: The overlapping supports of α and its translates over a lattice. The lightest regions correspond to Ω, points of which are covered by a unique translate of the atom α.

2. **Analysis of symmetry** By the *symmetry* of an atom α, we mean the group of transformations of the plane that leave α invariant,

$$\mathcal{G}_\alpha = \left\{ \text{isometries } g \text{ of } \mathbf{R}^2 \;\middle|\; \alpha \circ g = \alpha \right\}.$$

Note that any set defined in terms of α gets mapped onto itself by every $g \in \mathcal{G}_\alpha$. In particular, $K = \operatorname{supp}\alpha$ and $L = \mathbf{R}^2 - \alpha^{-1}(1)$ are fixed sets, and the centroid c of $\operatorname{supp}\alpha$ is a fixed point, of $\mathcal{G}_\alpha$. Without loss of generality, we may assume that the centroid is the origin, making each $g \in \mathcal{G}_\alpha$ linear.

Given a lattice $\mathcal{L}$ in the plane, we write $\operatorname{Aut}\mathcal{L}$ for the group of transformations of the plane that leave $\mathcal{L}$ invariant,

$$\operatorname{Aut}\mathcal{L} = \left\{ \text{isometries } g \text{ of } \mathbf{R}^2 \mid \forall l \in \mathcal{L}, g(l) \in \mathcal{L} \right\}.$$

Our main result in this section is to show that if α is the atom of a partition of unity based on the lattice $\mathcal{L}$, then

$$\mathcal{G}_\alpha \subseteq \operatorname{Aut}\mathcal{L}. \tag{2}$$

To facilitate the proof of this result, we introduce some notions that pertain to convex sets generally. The unit circle $S^1 \subset \mathbf{R}^2$ provides a natural representation of directions in $\mathbf{R}^2$. Letting λ be a supporting line of a convex set $K \subset \mathbf{R}^2$ having direction $z \in S^1$, we say that λ is *positively oriented supporting line* of K if, with respect to z, K lies to the left of λ.

DEFINITION 1. The *supporting line relation* of a convex set $K \subset \mathbf{R}^2$ is the set $R_K \subset S^1 \times \partial K$ consisting of pairs (z,p) such there is a supporting line of K through p in the direction z that is positively oriented with respect to z. (See Figure 2.)

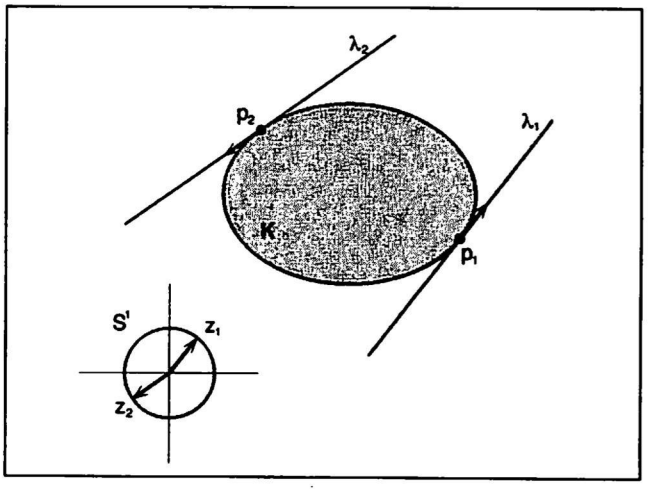

Figure 2: The pairs (z_1, p_1) and (z_2, p_2) belong to the supporting line relation R_K.

Writing π_{S^1} and $\pi_{\partial K}$ for the natural projections on $S^1 \times \partial K$, it is easy to see that $\pi_{S^1}: R_K \to S^1$ is surjective if K is compact, and that $\pi_{\partial K}: R_K \to \partial K$ is surjective unconditionally. If K is compact and strictly convex, then R_K is the graph of a function f_K on S^1. (In strict, set-theoretic terms, the relation R_K itself is a function, however we prefer to work with a separate symbol.)

DEFINITION 2. Given a compact, strictly convex set $K \subset \mathbf{R}^2$, the *supporting line function* of K is the map $f_K: S^1 \to \partial K$, where, for every $z \in S^1$, $p = f_K(z)$ is the unique point in the boundary of K such that $(z,p) \in R_K$.

Letting $K + u$ denote the translate of K by $u \in \mathbf{R}^2$, observe that

$$R_{K+u} = \{(z, p+u) \mid (z,p) \in R_K\},$$

so that if K is compact and strictly convex,

$$(z,p) \in R_{K+u} \implies u = p - f_K(z). \tag{3}$$

A local version of the supporting line relation can be applied to arbitrary sets in $\mathbf{R}^2$, as follows.

DEFINITION 3. Given an arbitrary set $L \subset \mathbf{R}^2$, the *local supporting line relation* of L is the set R_L^{loc}, consisting of pairs $(z,p) \in S^1 \times \partial L$ such that, for sufficiently small $\epsilon > 0$, $B_\epsilon(p) \cap L$ is convex and $(z,p) \in R_{B_\epsilon(p) \cap L}$. (See Figure 3.)

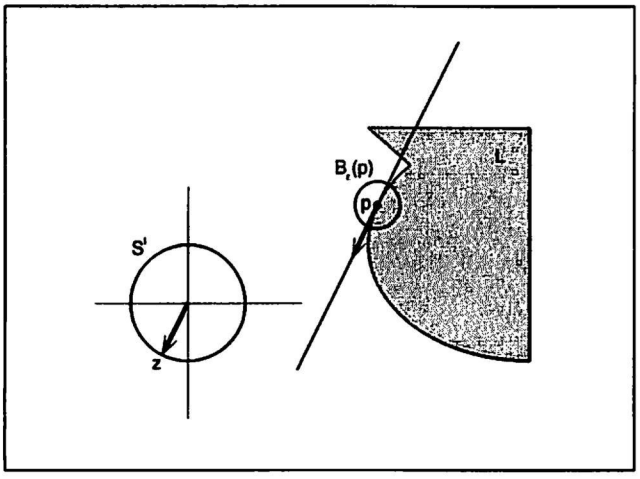

Figure 3: The pair (z,p) belongs to the local supporting line relation R_L^{loc}.

Of course for a convex set K, $R_K^{\text{loc}} = R_K$.

Now let us consider the sets $K = \operatorname{supp}\alpha$ and $L = \mathbf{R}^2 - \alpha^{-1}(1)$, where α is the atom of a partition of unity and the centroid of K is $c = (0,0)$. A simple, but key, observation is that

$$R_L^{\mathrm{loc}} \subset \bigcup_{l \in \mathcal{L}} R_{K+l}, \tag{4}$$

which follows from the fact the $\sum_{l \in \mathcal{L}} \alpha(x - l) = 1$. (See Figure 4.) Since K is strictly convex, (4) and (3) imply that

$$(z,p) \in R_L^{\mathrm{loc}} \implies p - f_K(z) \in \mathcal{L}. \tag{5}$$

Let $\mathcal{N} \subset \mathcal{L}$ denote the *neighbours* of the centroid $c = (0,0)$ of K, defined to be the set of points of the form

$$n = p - f_K(z), \qquad (z,p) \in R_L^{\mathrm{loc}}.$$

(See Figure 4.) If $u \neq 0$, then $\partial K \cap \partial(K + u)$ consists of at most two points, by strict convexity of K. Therefore all but finitely many points of ∂L belong to the boundary of a unique translate of K, and $\pi_{\partial L}(R_L^{\mathrm{loc}})$ includes all but finitely many points of ∂L.

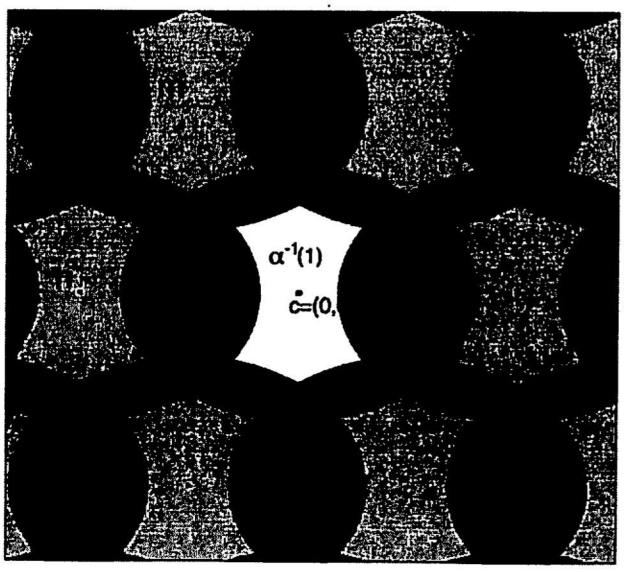

Figure 4: The set L is the region lying outside the curved hexagon enclosing $\alpha^{-1}(1)$. The vertices of this hexagon are the only points of ∂L *not* in $\pi_{\partial L}(R_L^{\mathrm{loc}})$. The lattice points included in the figure (apart from c itself) are precisely the neighbours of c.

LEMMA 1. *If $g \in \mathcal{G}_\alpha$ then $g(\mathcal{N}) = \mathcal{N}$.*

PROOF. Note that if $g \in \mathcal{G}_\alpha$, then $f_K \circ g = g \circ f_K$. Also,

$$R_L^{\text{loc}} = R_{g(L)}^{\text{loc}} = \{(g(z), g(p)) \mid (z,p) \in R_L^{\text{loc}}\}. \tag{6}$$

Now, if $n \in \mathcal{N}$, then

$$\begin{aligned} g(n) &= g(p - f_K(z)) && \text{(for some } (z,p) \in R_L^{\text{loc}}) \\ &= g(p) - g(f_K(z)) \\ &= g(p) - f_K(g(z)) \\ &\in \mathcal{N} && \text{(by (6) and (5)).} \end{aligned}$$

■

LEMMA 2. *The span of $\mathcal{N}$ over $\mathbf{Z}$ is $\mathcal{L}$.*

PROOF. To begin, note that $d = |\mathcal{N}| \geq 3$. Fix $n_1 \in \mathcal{N}$ and order the elements of $\mathcal{N}$ by increasing angle about the origin, counterclockwise from n_1:

$$n_1, n_2, \ldots, n_d.$$

Convexity of K implies that no two neighbours of $c = (0,0)$ can lie in the same ray of a line through c, so the above ordering is uniquely determined. Since $d \geq 3$, there exist two consecutive neighbours, $m = n_i, n = n_{i+1}$, such that the angle from m to n is less than π (see Figure 4).

Now consider the closed, convex hull T of the triangle cmn. By construction, T does not contain any additional elements of $\mathcal{N}$ apart from its vertices. Observe furthermore that T does not contain any additional elements of $\mathcal{L}$. That is, the only lattice points belonging to T are its vertices, from which it follows that the only lattice points belonging to the parallelogram P determined by m, n are its vertices.

We claim that the $\mathbf{Z}$-span of $\{m, n\}$ is $\mathcal{L}$. To see this, let u, v generate $\mathcal{L}$ and let $A\colon \mathbf{R}^2 \to \mathbf{R}^2$ denote the transformation that maps u, v to the standard basis vectors e_1, e_2, respectively, so that A maps $\mathcal{L}$ onto $\mathbf{Z}^2$. Consider the quadratic form

$$\langle Ax, Ax \rangle, \tag{7}$$

where $\langle \cdot, \cdot \rangle$ is the usual Euclidean inner product. The parallelogram P determined by m, n has a lattice point at each vertex and no other lattice points in its closure—and translates of P tile $\mathbf{R}^2$. Therefore, with respect to the quadratic form (7), P has area 1. But this says exactly that

$$\det \begin{pmatrix} Am \\ An \end{pmatrix} = 1,$$

and so the integer matrix

$$\begin{pmatrix} Am \\ An \end{pmatrix}$$

is invertible over the integers. It follows that the $\mathbf{Z}$-span of $\{Am, An\}$ is $\mathbf{Z}^2$. Pulling back by A^{-1} yields that the $\mathbf{Z}$-span of $\{m, n\}$ is $\mathcal{L}$, as desired. ∎

It is now a straightforward matter to prove our main result.

THEOREM 1. $\mathcal{G}_\alpha \subseteq \operatorname{Aut} \mathcal{L}$.

PROOF: If $g \in \mathcal{G}_\alpha$ then g maps $\mathcal{N}$ into $\mathcal{L}$ by Lemma 1. But $\mathcal{N}$ generates $\mathcal{L}$ over $\mathbf{Z}$, by Lemma 2, and $\mathcal{L}$ is closed under integer combinations, so it follows that g maps $\mathcal{L}$ into $\mathcal{L}$. Since g is an isometry, this implies that $g \in \operatorname{Aut} \mathcal{L}$. ∎

Writing C_n for the cyclic group of order n, and D_n for the corresponding dihedral group, the complete list of linear automorphism groups of planar lattices is:

$$C_1, C_2, C_3, C_4, C_6;\ D_1, D_2, D_3, D_4, D_6.$$

(See [4, p. 102].) Note that by choosing the centroid of the atom α to lie at the origin $(0,0)$, $\mathcal{G}_\alpha$ belongs not just to $\operatorname{Aut} \mathcal{L}$, but to the subgroup consisting of *linear* automorphisms. Thus Theorem 1 implies that $\mathcal{G}_\alpha$ is one of the above groups. The largest of these groups is D_6, so D_6 represents the maximum possible symmetry of an atom. In the next section we show that this symmetry is attainable.

3. **An explicit example** Let $\mathcal{L}_6$ denote the lattice in $\mathbf{R}^2$ generated by the vectors

$$v_1 = (\sqrt{3}, 0), \qquad v_2 = (\sqrt{3}/2, 3/2).$$

Define $\varphi\colon \mathbf{R}^+ \to \mathbf{R}$ by

$$\varphi(t) = \begin{cases} 1 & 0 \le t \le 1 \\ \frac{1}{2} \tanh\left(\frac{t-3/2}{(t-1)(t-2)}\right) + \frac{1}{2} & 1 < t < 2 \\ 0 & 2 \le t < \infty, \end{cases}$$

and set

$$\alpha_6(x) = \frac{\varphi(x \cdot x)}{\sum_{l \in \mathcal{L}_6} \varphi((x-l)\cdot(x-l))}. \tag{8}$$

Note that α_6 is C^∞ and that $\mathcal{L}_6$ and α_6 satisfy equation (1) and the defining conditions (i)–(iii); in particular, $\alpha_6(x) = 1$ for $\|x\| < \sqrt{3} - \sqrt{2}$. Let us consider for a moment the symmetry of α. It is evident from the expression (8) that α_6 is invariant with respect to every linear isometry of $\mathbf{R}^2$ that induces an automorphism of $\mathcal{L}_6$. Observe that $(0,0), v_1$ and v_2 are the vertices of an equilateral

triangle, so that $\mathcal{L}_6$ is a regular hexagonal (honeycomb) lattice, whose automorphism group includes D_6. This means that the dihedral group D_6 is a subset of $\mathcal{G}_{\alpha_6}$. On the other hand, $\mathcal{G}_{\alpha_6} \subset \mathcal{L}_6$, by Theorem 1, and it follows that $\mathcal{G}_{\alpha_6} = D_6$, the maximum symmetry possible.

References

1. Hans G. Feichtinger and Thomas Strohmer, editors, *Advances in Gabor analysis*, Applied and Numerical Harmonic Analysis, Birkhaeuser, Boston, 2003.
2. Karlheinz Groechenig, *Foundations of time-frequency analysis*, Applied and Numerical Harmonic Analysis, Birkhauser, Boston, 2001.
3. Michael P. Lamoureux, Peter C. Gibson, Jeff P. Grossman and Gary F. Margrave, *A fast, discrete Gabor transform via a partition of unity*, 35pp., preprint.
4. Hermann Weyl, *Symmetry*, Princeton University Press, Princeton, 1952.

Mathematisches Institut II
Universität Karlsruhe
Englerstr. 2
76128 Germany
gibson@math.uni-karlsruhe.de

Department of Mathematics & Statistics
University of Calgary
Calgary AB, T2N 1N4
mikel@math.ucalgary.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. **26**, (3), 2004 pp. 73–78

A REMARK ON THE RANKS OF TWISTS OF ELLIPTIC CURVES

JUNG-JO LEE

Presented by M. Ram Murty, FRSC

ABSTRACT. Let $f(n)$ be the number of factorizations of $n = ab$ for which $a + b$ is a square. We can prove an estimate

$$\sum_{n \leq x} f(n) = Cx + O(x^{1/2})$$

for some constant C. This formula is a consequence of our study of ranks of elliptic curves.

RÉSUMÉ. Soit $f(n)$ le nombre de factorizations $n = ab$ pour laquelle $a + b$ est un carré. Nous démontrons une estimation

$$\sum_{n \leq x} f(n) = Cx + O(x^{1/2})$$

pour une constante C. Cette formule est une conséquence concernant les études des rangs des courbes elliptiques.

1. **Introduction** Let E be an elliptic curve defined by the Weierstrass equation

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Z}.$$

By a celebrated theorem of Mordell, the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group. The Nagell-Lutz Theorem and Mazur's Theorem provide a complete description of the torsion part of elliptic curves over $\mathbb{Q}$. See [4] Chapter II, §5 for details. However, its rank has been the study of numerous papers, and its behaviour is still unknown. More generally, Mordell-Weil Theorem states that elliptic curves over algebraic number fields have the same algebraic structure.

In 1960, Honda[2] made the following conjecture on the rank of elliptic curves.

CONJECTURE 1. (Honda) *For every elliptic curve E defined over a number field, there exists a constant $c(E)$ such that*

$$\operatorname{rank} E(k) \leqslant c(E)[k : \mathbb{Q}]$$

for every number field k of definition for E. ($[k : \mathbb{Q}]$ is the extension degree of k over $\mathbb{Q}$.)

Received by the editors on November 7, 2003.
AMS subject classification: 14H52, 11N37.

In particular, this conjecture implies that the rank of elliptic curves in a family of twists (quadratic, cubic, quartic, etc.) over $\mathbb{Q}$ is bounded by a constant.

On the other hand, many mathematicians expect that there might be elliptic curves of arbitrarily large ranks. There is an algorithm to get a lower bound for the rank of elliptic curves, which was used to obtain elliptic curves of large ranks in some papers such as [1] or [3]. In [3], the authors could produce several specific examples of elliptic curves with ranks at least six using this algorithm. In [1], D. Clark makes a conjecture which implies that there is a curve with rank larger than any given number.

CONJECTURE 2. (Clark) *Let*

$$f(n) = \#\{(a,b) \in \mathbb{Z} \times \mathbb{Z} : ab = n,\ a+b = \square\}.$$

Then

$$\limsup_{\substack{n\to\infty \\ n \text{ square-free}}} f(n) = +\infty.$$

The purpose of this paper is to remark that the general Honda's conjecture is incompatible with Clark's conjecture and improve the average order estimate of the related arithmetic function in Clark's paper. We explain this point in more detail below.

2. An Algorithm of Tate

Let's restrict our attention to elliptic curves of the form

$$E : y^2 = x^3 + ax^2 + bx,$$

where $a, b \in \mathbb{Z}$ and $a^2 - 4b$ is not a square.

Consider the mapping

$$\alpha_E : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$$

which is defined by

$$\alpha_E(x,y) = x\mathbb{Q}^{*2} \text{ if } x \neq 0, \quad \alpha_E(0,0) = b\mathbb{Q}^{*2}, \text{ and } \alpha_E(O) = \mathbb{Q}^{*2}.$$

It is known that α_E is a group homomorphism. For this homomorphism, see [4] Chapter III, §§5, 6. The following Theorems 3 and 4 can also be found from the same reference.

THEOREM 3. *Let r be the rank of E. Then we have that*

$$2^{r-1} \geqslant [\operatorname{Im} \alpha_E].$$

THEOREM 4.

$$\operatorname{Im}\alpha_E = \{b\mathbb{Q}^{*2}\} \cup \Big\{ b_1\mathbb{Q}^{*2} : b_1 \in \mathbb{Z}, b = b_1b_2, \text{ and } b_1M^4 + b_2e^4 + aM^2e^2 = N^2 \text{ has a solution } (M,e,N) \text{ in pairwise prime nonzero integers} \Big\}.$$

In their search for elliptic curves of large ranks, Penney and Pomerance [3] make a simplifying assumption that $M = e = 1$. Namely, they study

$$A = \{b\mathbb{Q}^{*2}\} \cup \{b_1\mathbb{Q}^{*2} : b_1 \in \mathbb{Z},\ b = b_1b_2,\ b_1 + b_2 + a \text{ is a nonzero square}\},$$

from which the relations

$$\begin{cases} b_1 + b_2 = N^2 - a, \\ b_1b_2 = b \end{cases}$$

follow. In this context, assuming further that the coefficient of the quadratic term vanishes, Clark defines the following arithmetic function associated with the rank of elliptic curves

$$f(n) = \#\{(a,b) \in \mathbb{Z} \times \mathbb{Z} : ab = n,\ a + b = \square\}.$$

LEMMA 5. *If $E : y^2 = x^3 + nx$ is an elliptic curve of rank r over $\mathbb{Q}$, with $n \in \mathbb{Z}$ square-free, then*

$$f(n) \leqslant 2^{r+2}.$$

PROOF. Every factorization $n = ab$, with $a + b = \square$, gives rise to two elements of $\operatorname{Im}\alpha_E$ by Theorem 4. So Theorem 3 implies the desired result. This is Theorem 1 of [1]. ∎

It is now obvious from the algorithm of Tate that if

$$\limsup_{\substack{n\to\infty \\ n \text{ square-free}}} f(n) = +\infty,$$

then elliptic curves with arbitrarily large rank can be found.

We now prove:

PROPOSITION 6. *The general Honda conjecture is incompatible with Clark's conjecture.*

PROOF. $y^2 = x^3 + nx$ are all quartic twists of $y^2 = x^3 + x$. Honda's conjecture says that the ranks are bounded by a constant in a family of quartic twists, whereas by Lemma 5 Clark's conjecture implies that there is an elliptic curve in this family whose rank is larger than any given number. ∎

Related to this, Clark [1] proved that

$$\limsup_{n\to\infty} f(n) = +\infty.$$

Let $E : y^2 = x^3 + Dx$ and $E_{R,Q} : y^2 = x^3 + DR^4Q^4x$ for some integers R and Q. He proved $\limsup_{n\to\infty} f(n) = +\infty$ in this family by choosing appropriate R and Q. But this cannot be used to construct a specific curve of large rank as the curves $E(\mathbb{Q})$ and $E_{R,Q}(\mathbb{Q})$ are the same curve under a birational change of coordinates.

3. **Average Order Estimate** Clark's paper can be considered as a first attempt to express the rank problem of elliptic curves in terms of properties of related arithmetic functions. We have a formula describing the average order of $f(n)$. Here, we provide an improved version of Theorem 3 of [1].

THEOREM 7.

$$\sum_{n\leqslant x} f(n) = C\cdot x^{\frac{3}{4}} + O(x^{\frac{1}{2}})$$

where $C = 2\int_0^1 \sqrt{\frac{1}{u}+u}\,du - \frac{4}{3} \approx 3.0244$.

PROOF. Recall the definition of $f(n)$ which was given by

$$f(n) = \#\{(a,b) : ab = n,\ a+b = \square\}.$$

Thus,

$$\begin{aligned}\sum_{n\leqslant x} f(n) &= \sum_{ab\leqslant x,\ a+b=\square} 1 = 2\sum_{a\leqslant\sqrt{x}} \sum_{0\leqslant b=m^2-a\leqslant\frac{x}{a}} 1\\ &= 2\sum_{a\leqslant\sqrt{x}} \sum_{\sqrt{a}\leqslant m\leqslant\sqrt{\frac{x}{a}+a}} 1\\ &= 2\sum_{a\leqslant\sqrt{x}} \left(\left[\sqrt{\frac{x}{a}+a}\right] - [\sqrt{a}]\right),\end{aligned}$$

where $[\,x\,]$ denotes the greatest integer less than or equal to x .

As

$$\sqrt{\frac{x}{a}+a} - \sqrt{a} - 1 \leqslant \left[\sqrt{\frac{x}{a}+a}\right] - [\sqrt{a}] \leqslant \sqrt{\frac{x}{a}+a} - \sqrt{a} + 1$$

we have

$$\sum_{n\leqslant x} f(n) = 2\sum_{a\leqslant\sqrt{x}} \left(\sqrt{\frac{x}{a}+a} - \sqrt{a}\right) + O(x^{\frac{1}{2}}).$$

Now, notice that the functions

$$\sqrt{\frac{x}{a}+a} \quad \text{and} \quad \sqrt{a}$$

are monotonic on the interval $[1, \sqrt{x}]$, taking maximum $\sqrt{x+1}$ at $a=1$ and minimum $\sqrt{2\sqrt{x}}$ at $a=\sqrt{x}$, and maximum $\sqrt[4]{x}$ at $a=\sqrt{x}$ and minimum 1 at $a=1$, respectively. Therefore,

$$\left| \sum_{a \leqslant \sqrt{x}} \sqrt{\frac{x}{a}+a} - \int_1^{\sqrt{x}} \sqrt{\frac{x}{a}+a}\, da \right| \leqslant \sqrt{x+1} - \sqrt{2\sqrt{x}} = O(x^{\frac{1}{2}})$$

and

$$\left| \sum_{a \leqslant \sqrt{x}} \sqrt{a} - \int_1^{\sqrt{x}} \sqrt{a}\, da \right| \leqslant \sqrt[4]{x} - 1 = O(x^{\frac{1}{4}}).$$

Thus,

$$\begin{aligned} \sum_{n \leqslant x} f(n) &= 2\int_1^{\sqrt{x}} \sqrt{\frac{x}{a}+a}\, da - 2\int_1^{\sqrt{x}} \sqrt{a}\, da + O(x^{\frac{1}{2}}) \\ &= 2\int_1^{\sqrt{x}} \sqrt{\frac{x}{a}+a}\, da - \frac{4}{3}x^{\frac{3}{4}} + O(x^{\frac{1}{2}}). \end{aligned}$$

To estimate the remaining integral, we change the variable by $a = \sqrt{x}u$, then

$$\begin{aligned} \sum_{n \leqslant x} f(n) &= 2\int_{\frac{1}{\sqrt{x}}}^1 \sqrt{\frac{x}{\sqrt{x}u}+\sqrt{x}u}\, \sqrt{x} du - \frac{4}{3}x^{\frac{3}{4}} + O(x^{\frac{1}{2}}) \\ &= 2 \cdot x^{\frac{3}{4}} \int_{\frac{1}{\sqrt{x}}}^1 \sqrt{\frac{1}{u}+u}\, du - \frac{4}{3}x^{\frac{3}{4}} + O(x^{\frac{1}{2}}) \\ &= \left(2\int_{\frac{1}{\sqrt{x}}}^1 \sqrt{\frac{1}{u}+u}\, du - \frac{4}{3}\right) \cdot x^{\frac{3}{4}} + O(x^{\frac{1}{2}}) \\ &= \left(2\int_0^1 \sqrt{\frac{1}{u}+u}\, du - 2\int_0^{\frac{1}{\sqrt{x}}} \sqrt{\frac{1}{u}+u}\, du - \frac{4}{3}\right) \cdot x^{\frac{3}{4}} + O(x^{\frac{1}{2}}). \end{aligned}$$

Here,

$$\int_0^{\frac{1}{\sqrt{x}}} \sqrt{\frac{1}{u}+u}\, du \leqslant \int_0^{\frac{1}{\sqrt{x}}} \left(\sqrt{\frac{1}{u}} + \sqrt{u}\right) du = 2x^{-\frac{1}{4}} + \frac{2}{3}x^{-\frac{3}{4}} = O(x^{-\frac{1}{4}}).$$

So

$$\sum_{n\leqslant x} f(n) = \left(2\int_0^1 \sqrt{\frac{1}{u}+u}\,du + O(x^{-\frac{1}{4}}) - \frac{4}{3}\right)\cdot x^{\frac{3}{4}} + O(x^{\frac{1}{2}})$$

$$= \left(2\int_0^1 \sqrt{\frac{1}{u}+u}\,du - \frac{4}{3}\right)\cdot x^{\frac{3}{4}} + O(x^{\frac{1}{2}}).$$

This completes the proof. ∎

Acknowledgements. I would like to thank Professor Ram Murty for comments and suggestions.

REFERENCES

[1] D. Clark, *An arithmetical function associated with the rank of elliptic curves*, Canad. Math. Bull. **34** (1991), 181–185.
[2] T. Honda, *Isogenies, rational points and section points of group varieties*, Jap. Journal of Math. **30** (1960), 84–101.
[3] E. Penney and C. Pomerance, *A search for elliptic curves with large rank*, Math. Comp. **28** (1974), 851–853.
[4] J. Silverman and J. Tate, *Rational points on elliptic curves*, UTM, Springer-Verlag, New York, 1992

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
K7L 3N6
email: jjlee@mast.queensu.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. 26, (3), 2004 pp. 79–83

VIRTUALLY FREE PRO-P GROUPS

W. HERFORT AND P. A. ZALESSKII

Presented by Vlastimil Dlab, FRSC

RÉSUMÉ. Nous étudions la classe des groupes pro-p avec un sous-groupe ouvert et pro-p libre. Nous montrons que tout ce groupe opère sur un arbre pro-p qui a des stabilisateurs de points finis. Il s'agit d'une généralisation du resultat bien connu de J.-P. Serre, que tout ce groupe pro-p sans torsion est un groupe pro-p libre.

Par conséquence, nous décrivons quelques sous-groupes finis du groupe des automorphismes d'un groupe pro-p libre engendré par une partie finie.

ABSTRACT. Virtually free pro-p groups are described. This generalizes Serre's result, stating that a torsion free virtually free pro-p group is free pro-p.

As a consequence of our main result certain finite subgroups and their conjugacy classes in the automorphism group of a finitely generated free pro-p group are classified.

1. Introduction Let p be a prime number, and G a pro-p group containing an open free pro-p subgroup F. If G is torsion free, then, according to the celebrated theorem of Serre in [9], G itself is free pro-p.

The main objective of the paper is to announce the description of virtually free pro-p groups without the assumption of torsion freeness.

THEOREM 1. *A virtually free pro-p group acts on a pro-p tree with finite vertex stablilizers of bounded order.*

Having Bass-Serre theory (in the discrete situation) in mind, Theorem 1 is the pro-p analogue of the description of virtually free discrete groups proved by Karrass, Pietrovski and Solitar [5] for the finitely generated case, Cohen [1] for countably generated groups and Scott [8] in the general situation. However in contrast to the discrete situation, for a pro-p group G to act on a pro-p tree T is a weaker property than to be the fundamental group of the corresponding profinite graph of pro-p groups. The reason is that in the pro-p situation a maximal subtree of T/G does not always exist, and even when it exists not always lifts to T. When the maximal subtree of T/G exists and lifts to T, the aforementioned properties are equivalent.

In Theorem 1 maximal finite subgroups of G are exactly stabilizers of vertices and conjugated finite subgroups stabilize vertices of the same orbit respectively. So if a virtually free pro-p group G has only finitely many conjugacy classes of finite subgroups (to be termed a CFG-group), then T/G has only finitely many

Received by the editors on November 17, 2003.
Pavel Zalesskii expresses his thanks for support through CNPq.
AMS subject classification: 20E18.

vertices and so contains a maximal finite subtree. This allows us to characterize a virtually free pro-p CFG-group as the fundamental group of a graph of finite p-groups, and in particular, we obtain the following description of finitely generated virtually free pro-p groups.

THEOREM 2. *A finitely generated pro-p group G is a virtually free pro-p group if and only if G is isomorphic to the fundamental group $\Pi_1(\mathcal{G}, \Gamma, T)$ of a finite graph of finite p-groups. In particular, it is the pro-p completion of some finitely generated dense virtually free subgroup.*

It should be mentioned that we obtain the last statement of this theorem as a consequence of Theorem 1; the discrete result is not used (and cannot be used) during the proof. In the characterization of discrete virtually free groups Stallings' *theory of ends* played a crucial role. In fact the proof of the Theorem of Karrass-Pietrovski-Solitar, Cohen and Scott uses the celebrated Theorem of Stallings in [10], according to which every virtually free group splits as an amalgamated free product/HNN-extension over a finite group. Note that a theory of ends has not been developed in the pro-p situation.

Thus purely combinatorial pro-p group methods are used in the present paper for proving our main result and the following pro-p version of Stallings' Theorem.

THEOREM 3. *Let G be a finitely generated virtually free pro-p group. Then G is either a non-trivial amalgamated free pro-p product with finite amalgamating subgroup or it is a non-trivial HNN-extension with finite associated subgroups.*

We also announce an example of a split extension $H = F \rtimes D_4$ of a free pro-2 group F of countable rank, which can not be represented as the fundamental pro-2 group of a profinite graph of finite 2-groups showing that Theorem 2 cannot be extended to a general situation. Moreover, one can embed H into an amalgamated free pro-2 product $D_4 \amalg_{C_2} (C_2 \times C_2)$. This shows that a pro-$p$ analogue of Bass-Serre's Theorem (Theorem 6.1 in [2]) does not hold for arbitrary closed subgroups of an amalgamated free pro-p product.

V. A. Romankov proved in [7] that (in contrast to the discrete situation) the automorphism group of a finitely generated free pro-p group of rank ≥ 2, is infinitely generated. Nevertheless, Theorem 1 allows us to obtain (see Theorem 6) a description of the conjugacy classes of finite p-groups of the automorphism group of a finitely generated free pro-p group (see Theorem 7).

Basic material on profinite groups can be found in [11, 6]. The notions of *fundamental group of a graph of pro-p groups* and fundamental pro-p group of a profinite graph can be found e.g. in [12, 13]. By $\mathrm{Tor}(G)$ we mean the subset of elements of finite order in G.

2. Ingredients

The following very recent result of the second author [14] is crucial.

PROPOSITION 4. *Let G be any virtually free pro-p group and $N \lhd G$ arbitrary with $N = \langle Tor(N)\rangle$. Then the following statements hold:*

(i) *$Tor(G/N) = Tor(G)N/N$ (torsion from G/N can be lifted).*
(ii) *$G/\langle Tor(G)\rangle$ is free pro-p.*

When the graph Γ contains a spanning tree T (e.g. when its set of vertices is finite), the following description along the lines of discrete group theory can be given.

DEFINITION 5 A profinite graph of pro-p groups $(\mathcal{G}, \Gamma, T)$ is defined as follows. Given a profinite graph Γ containing a maximal tree T and a profinite space $\mathcal{G}$ together with a continuous surjective map $\gamma\colon \mathcal{G} \to \Gamma$ such that every fiber $\mathcal{G}(t) := \gamma^{-1}(t)$ is a pro-p group. The operations of group multiplication, wherever defined on $\mathcal{G} \times \mathcal{G}$, and inversion of elements, are both continuous. There are continuous maps $\partial_i\colon \mathcal{G} \to \gamma^{-1}(V(\Gamma))$ for $i = 0, 1$ such that the restriction to every fiber is a group monomorphism and ∂_i is the identity on $\gamma^{-1}(V(\Gamma))$. Moreover $\gamma\partial_i = d_i\gamma$ holds for $i = 0, 1$.

A presentation of the fundamental pro-p group of the profinite graph of pro-p groups $(\mathcal{G}, \Gamma, T)$ is then as follows:

$$\Pi_1(\mathcal{G}, \Gamma, T) \cong \Big\langle \mathcal{G}(v), g_e \;\Big|\; \mathrm{rel}(\mathcal{G}(v)), v \in V(\Gamma);\ \partial_0(g) = \partial_1(g)^{g_e}, \in \mathcal{G}(e), e \in E(\Gamma);\ g_e = 1, e \in E(T)\Big\rangle.$$

The following notions play a role during the induction proof of Theorem 1:

NOTATION 1. For a virtually free pro-p group G let $\mathbf{n}(G)$ be minimal among all natural numbers k such that G possesses a normal open free pro-p subgroup of index p^k. Define a function **ord** from the class of all virtually free pro-p groups to $\mathbf{N}$ by setting

$$\mathbf{ord}(G) := \mathbf{n}(G/\mathrm{Z}(G))$$

for any virtually free pro-p group G.

The proof of Theorem 1 is performed by induction on $\mathbf{ord}(G)$ and uses that centralizers of elements of order p in G satisfy the induction hypothesis. A basis of the induction is the situation when G is the extension of a free pro-p group by a cyclic group of order precisely p. This special case has been treated separately in [4].

Proof of Theorem 3: Theorem 2 shows the existence of a finite graph $(\mathcal{G}, \Gamma)$ of finite p-groups with $G = \Pi_1(\mathcal{G}, \Gamma)$. Choose an arbitrary edge e of Γ. If $\Delta := \Gamma \setminus \{e\}$ is connected, then clearly $G = HNN(H, G_e, t)$ is an HNN-extension, where $H = \Pi_1(\mathcal{G}_{|\Delta}, \Delta)$. If Δ is not connected, then $G = H_1 \amalg_{G_e} H_2$, where $H_i = \Pi_1(\mathcal{G}_{|C_i}, C_i)$ with C_i $(i = 1, 2)$ denoting the connected components of Δ. ∎

3. **Consequences** For a finite set X the canonical embedding of the discrete free group $\Phi(X)$ into its pro-p-completion $F(X)$ induces an embedding $\mathrm{Aut}(\Phi(X)) \leq \mathrm{Aut}(F(X))$.

THEOREM 6. *Let $F = F(X)$ be a finitely generated free pro-p group and $\Phi = \Phi(X)$ be a dense abstract free subgroup of F on the same set of generators. Suppose that $A \leq \mathrm{Aut}(F)$ is a finite p-group. Then there exists an automorphism $\beta \in \mathrm{Aut}(F)$ such that in $\mathrm{Aut}(F)$, the conjugate $A^\beta \leq \mathrm{Aut}(\Phi)$.*

PROOF. Use Theorem 2 in order to find $(\mathcal{G}, \Gamma)$ for the finitely generated virtually free pro-p group $G = F \rtimes A$. We consider G as a subgroup of $\mathrm{Aut}(F)$ and identify F with the group of inner automorphisms. Theorem 5.6 of [12] then shows that there exists $\beta_0 \in G$ with $A^{\beta_0} \in G(v)$ for some $v \in V(\Gamma)$. Let $\pi_1(\mathcal{G}, \Gamma)$ be the abstract fundamental pro-p group (see, e.g., [2]), and put $\Phi_0 := \pi_1(\mathcal{G}, \Gamma) \cap F$. Choose a basis Y of Φ_0. Then Y is a basis of $F(X)$, thus there exists $\alpha \in \mathrm{Aut}(F(X))$ sending X bijectively to Y. For $\beta := \beta_0\alpha$, $A^\beta \leq \mathrm{Aut}(\Phi)$. ∎

THEOREM 7. *Let Φ be a free group of rank n and $\hat{F}$ be its pro-p completion. Let $F^* := F^p[F, F]$ denote the Frattini subgroup o F.*

(i) *The natural embedding $\mathrm{Aut}(\Phi) \leq \mathrm{Aut}(F)$ induces a surjection of the set conjugacy classes of finite p-subgroups of $\mathrm{Aut}(\Phi)$ to the set of conjugacy classes of finite p-subgroups of $\mathrm{Aut}(F)$.*

(ii) *The $\mathrm{Aut}(F)$-conjugacy classes of finite subgroups of $\mathrm{Aut}(F)$ of order coprime to p are in one-to-one correspondence with $\mathrm{Aut}(F/F^*)$-conjugacy classes of finite subgroups of $\mathrm{Aut}(F/F^*) \cong GL_n(\mathbf{F}_p)$ of order coprime to p.*

PROOF. Statement (i) is a consequence of Theorem 6. We begin the proof of (ii) by defining a homomorphism $\psi\colon \mathrm{Aut}(F) \to \mathrm{Aut}(F/F^*)$ as follows:

$$\psi(\alpha)(fF^*/F^*) := \alpha(f)F^*/F^*.$$

Claim 1: *If, for finite p-groups $A, B \leq \mathrm{Aut}(F)$, $\psi(A)$ and $\psi(B)$ are conjugate in $\mathrm{Aut}(F/F^*)$, then A and B are conjugate in $\mathrm{Aut}(F)$.*

Suppose this is false. Then, by replacing B by a suitable conjugate in $\mathrm{Aut}(F)$, we can assume that A and B induce the same automorphism on F/F^*. Consider $L := F \rtimes A$, where F has been identified with its inner automorphism group. By Theorem 2.3.15 in [6] (a profinite version of the Schur-Zassenhaus Theorem), A and B are then conjugate in L, a contradiction.

Claim 2: *For every $A \leq \mathrm{Aut}(F)$ with order coprime to p, $\psi(A) \cong A$.*

It suffices to show that every nontrivial $\alpha \in A$ induces a nontrivial automorphism of F/F^*. Suppose now that α induces the identity on F/F^*. By

Proposition 2.3.16 in [6] we can find a generating set X of F with $x^\alpha = x$ for $x \in X$, whence α is the identity.

Claims 1 and 2 together yield (ii). ∎

We remark that (ii) of Theorem 7 generalizes a result of W. Herfort and L. Ribes: [3, Corollary 2.5].

References

1. D. E. Cohen, *Groups with free subgroups of finite index*, in: Conference on Group Theory, University of Wisconsin-Parkside 1972, Lecture Notes in Mathematics **319** Springer (1973), 26–44.
2. W. Dicks, *Groups, Trees and Projective Modules*, Springer 1980.
3. W. Herfort and L. Ribes, *On automorphisms of free pro-p groups I*, Proc. AMS **108** (1990) 287–295.
4. W. Herfort, L. Ribes and P. A. Zalesskii, *p extensions of free pro-p groups*, Forum Mathematicum **11** (1999) 49–61.
5. A. Karrass, A. Pietrovski and D. Solitar, *Finite and infinite cyclic extensions of free groups*, J. Australian Math. Soc. **16** (1973) 458–466.
6. L. Ribes and P. A. Zalesskii, *Profinite Groups*, Springer 2000.
7. L. Roman'kov, *Infinite generation of automorphism groups of free pro-p groups*, Siberian Mathematical Journal **34**, (1993) 727–732.
8. G. P. Scott, *An embedding theorem for groups with a free subgroup of finite index*, Bull. London Math. Soc. **6** (1974) 304–306.
9. J.-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology **3**, (1965) 413–420.
10. J. R. Stallings, *On torsion-free groups with infinitely many ends*, Ann. of Math. II. Ser. **88** (1968) 312–334.
11. J. S. Wilson, *Profinite Groups*, London Math. Soc. Monographs (Clarendon Press, Oxford, 1998)
12. P. A. Zalesskii and O. V. Mel'nikov, *Fundamental Groups of Graphs of Profinite Groups*, Algebra i Analiz **1** (1989); translated in: Leningrad Math. J. **1** (1990), 921–940.
13. P. A. Zalesskii and O. V. Mel'nikov, *Subgroups of profinite groups acting on trees*, Math. USSR Sbornik **63** (1989) 405–424.
14. P. A. Zalesskii, *Virtually projective groups*, J. für die Reine und Angewandte Mathematik (Crelle's Journal) (to appear).

University of Technology at Vienna
Vienna
Austria
email: w.herfort@tuwien.ac.at

University of Brasilia
Brasilia-DF
Brazil
email: pz@mat.unb.br

C. R. Math. Rep. Acad. Sci. Canada Vol. 26, (3), 2004 pp. 84–89

LIE TORI

ERHARD NEHER

Presented by R. V. Moody, FRSC

RÉSUMÉ. On annonce ici quelques résultats concernant les tores de Lie nécessaires à la construction des algèbres de Lie affines étendues dans [15].

ABSTRACT. We announce some results on Lie tori which are used in the description of extended affine Lie algebras in the following article [15].

0. Introduction. Lie tori are a class of Lie algebras that arise in the construction of extended affine Lie algebras; see the following article [15]. Examples of Lie tori are the loop algebras of finite-dimensional split simple Lie algebras; more examples are given in 4 below.

An important property of a Lie torus L is that L is graded by a finite irreducible root system Δ. Although one knows the structure of root-graded Lie algebras in general (Allison-Benkart-Gao [2], Berman-Moody [11], Benkart-Smirnov [7], Benkart-Zelmanov [8] and Neher [16]), it is non-trivial to characterize those that are Lie tori. As of now, the precise structure of a centreless Lie torus L has been worked out for the case of a reduced Δ and in a special case for $\Delta = \mathrm{BC}_1$ (see 4 for a summary).

In this note we announce some results on Lie tori that are needed for the description of extended affine Lie algebras: A Lie torus L is finitely generated as Lie algebra and the dimension of its homogeneous components are uniformly bounded (Theorem 5). The centroid $\mathrm{Cent}(L)$ of a centreless Lie torus L is always a Laurent polynomial ring, and if Δ is not of type A then L is a free $\mathrm{Cent}(L)$-module of finite rank (Theorem 7); the derivation algebra of L is a semidirect product of the ideal of inner derivations and the subalgebra of centroidal derivations (Theorem 9).

Details of proofs will appear elsewhere. The author thanks Bruce Allison and Yoji Yoshii for having provided him with their preprints [5], [19] and [23].

1. Notations and terminology. All vector spaces and algebras considered in this note will be defined over a field F of characteristic 0, except when indicated otherwise. For an abelian group G and a subset $R \subset G$ we denote by $\langle R \rangle$ the subgroup generated by R. Root systems will always contain 0. This has some notational advantages and follows the conventions in [1]. We will call Δ a finite root system if $\Delta^\times := \Delta \setminus \{0\}$ is a root system in the sense of [12, Ch.VI, §1.1]. In particular, Δ need not be reduced. For $\alpha, \beta \in \Delta$ we denote by $\langle \alpha, \beta^\vee \rangle$ the Cartan

Received by the editors on November 15, 2003.
Partial support by a NSERC (Canada) discovery grant is gratefully acknowledged.
AMS subject classification: Primary 17B65; Secondary 17B67, 17B70.

integer of α, β (thus $\langle \alpha, \beta^\vee \rangle = n(\alpha, \beta)$ in the notation of [12]) and by $\mathcal{Q}(\Delta) = \langle \Delta \rangle$ the root lattice of Δ. We denote by $\Delta_{\text{ind}} = \{0\} \cup \{\alpha \in \Delta^\times : \alpha/2 \notin \Delta\}$ the subsystem of indivisible roots of Δ.

2. Definition. Let Δ be a finite irreducible root system and let Λ be a free abelian group of finite rank. A *Lie torus of type* (Δ, Λ) is a Lie algebra L satisfying the following axioms:

(LT1) L has a $(\mathcal{Q}(\Delta) \oplus \Lambda)$-grading of the form

$$L = \bigoplus_{\alpha \in \mathcal{Q}(\Delta),\, \lambda \in \Lambda} L_\alpha^\lambda, \quad [L_\alpha^\lambda, L_\beta^\mu] \subset L_{\alpha+\beta}^{\lambda+\mu}, \quad \text{and } L_\alpha^\lambda = 0 \text{ if } \alpha \notin \Delta. \tag{2.1}$$

(LT2) For $\alpha \in \Delta^\times$ and $\lambda \in \Lambda$ we have

(i) $\dim L_\alpha^\lambda \leq 1$, with $\dim L_\alpha^0 = 1$ if $\alpha \in \Delta_{\text{ind}}$,

(ii) if $\dim L_\alpha^\lambda = 1$ then there exists $(e_\alpha^\lambda, f_\alpha^\lambda) \in L_\alpha^\lambda \times L_{-\alpha}^{-\lambda}$ such that $h_\alpha^\lambda = [e_\alpha^\lambda, f_\alpha^\lambda] \in L_0^0$ acts on $x_\beta^\mu \in L_\beta^\mu$ $(\beta \in \Delta, \mu \in \Lambda)$ by $[h_\alpha^\lambda, x_\beta^\mu] = \langle \beta, \alpha^\vee \rangle x_\beta^\mu$.

(LT3) For $\lambda \in \Lambda$ we have $L_0^\lambda = \sum_{\alpha \in \Delta^\times, \mu \in \Lambda} [L_\alpha^\mu, L_{-\alpha}^{\lambda-\mu}]$.

(LT4) $\Lambda = \langle \{\lambda \in \Lambda : L_\alpha^\lambda \neq 0 \text{ for some } \alpha \in \Delta\} \rangle$.

The rank of Λ is called the *nullity* of L. If (Δ, Λ) is not important or clear from the context, we will simply call L a *Lie torus*. Similarly, a Lie torus of type Δ and nullity n is a Lie torus of type (Δ, Λ) for some Λ of rank n.

Examples of Lie tori will be given in 4 below. It will emerge that Lie tori can be constructed using certain Λ-graded algebras, like Jordan, alternative or structurable algebras, which have been called Jordan tori, alternative tori or structurable tori respectively. This, together with the fact that toroidal Lie algebras are one of the main examples of Lie tori, is the justification for the name "Lie torus".

It is natural to consider Lie tori for more general groups Λ and with less restrictive conditions as (LT2i); see [21], [22] and [23] for some work in this direction. However, the results stated below require the axioms above.

3. Some properties of Lie tori. Let L be a Lie torus of type (Δ, Λ). Then L has a Λ-grading

$$L = \bigoplus_{\lambda \in \Lambda} L^\lambda, \quad L^\lambda := \bigoplus_{\alpha \in \Delta} L_\alpha^\lambda \tag{3.1}$$

as well as a $\mathcal{Q}(\Delta)$-grading

$$L = \bigoplus_{\alpha \in \Delta} L_\alpha, \quad L_\alpha := \bigoplus_{\lambda \in \Lambda} L_\alpha^\lambda. \tag{3.2}$$

The subalgebra $\mathfrak{g}$ of L^0 generated by $\{L^0_\alpha : \alpha \in \Delta^\times\}$ is a finite-dimensional split simple Lie algebra of type Δ_{ind} with splitting Cartan subalgebra

$$\mathfrak{h} = \sum_{\alpha \in \Delta^\times} [L^0_\alpha, L^0_{-\alpha}]. \tag{3.3}$$

With respect to $\mathfrak{g}$, $\mathfrak{h}$ and the decomposition (3.2), L is a Δ-graded Lie algebra; see [11], [8] or [16] for the case of a reduced Δ and [2], [7] for the case $\Delta = \mathrm{BC}$. It is then easily seen that our definition of a Lie torus is equivalent to the one given in [23] and [19]. A Lie torus is called *centreless* if its centre $Z(L)$ vanishes.

Let $C \subset Z(L) = \bigoplus_{\lambda \in \Lambda} (Z(L) \cap L^\lambda)$ be a Λ-graded subspace of $Z(L)$. Then L/C is canonically a Lie torus of type (Δ, Λ). In particular, $L/Z(L)$ is a centreless Lie torus. Conversely, the universal central extension of a Lie torus (more generally, any Λ-cover of L in the sense of [17, 1.15]) is again a Lie torus.

4. Examples. (a) Let $\mathfrak{g}$ be a finite-dimensional split simple Lie algebra of type Δ, and let $F[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$ be the ring of Laurent polynomials in n variables. Then $\mathfrak{g} \otimes F[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$ is a centreless Lie torus of type Δ and nullity n. Hence, by **3**, its universal central extension, i.e., the associated *toroidal Lie algebra* [14], is also a Lie torus of type Δ and nullity n. Conversely, by [9, Theorem 1.37], every Lie torus of type $\Delta = \mathrm{D}_l$, $l \geq 4$, or $\Delta = \mathrm{E}_l$, $l = 6, 7, 8$ and nullity n is a central extension of $\mathfrak{g} \otimes F[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$.

(b) The special case $n = 1$ and $F = \mathbb{C}$ of example (a) is worth pointing out. Then the *loop algebra* $L(\mathfrak{g}) = \mathfrak{g} \otimes \mathbb{C}[t^{\pm 1}]$ and its universal central extension $\hat{L}(\mathfrak{g})$ are Lie tori of nullity 1. More generally, it follows from the proof of [3, Theorem 1.19] that the complex Lie tori of nullity 1 are precisely the derived affine Lie algebras and their central quotients.

(c) Let $\mathbf{q} = (q_{ij}) \in \mathrm{M}_n(F)$ be a $(n \times n)$-matrix over F satisfying $q_{ii} = 1 = q_{ij} q_{ji}$ for $1 \leq i, j \leq n$, and let $F_\mathbf{q}$ be the associated *quantum torus*, which, by definition, is the unital associative algebra with $2n$ generators $t_1^{\pm 1}, \dots, t_n^{\pm 1}$ and defining relations $t_i t_i^{-1} = 1 = t_i^{-1} t_i$ and $t_i t_j = q_{ij} t_j t_i$ for $1 \leq i, j \leq n$. Denote by $[F_\mathbf{q}, F_\mathbf{q}]$ the span of all commutators $[a, b] = ab - ba$ with $a, b \in F_\mathbf{q}$. Then $\mathfrak{sl}_{l+1}(F_\mathbf{q}) = \{x \in \mathrm{M}_{l+1}(F_\mathbf{q}) : \mathrm{tr}(x) \in [F_\mathbf{q}, F_\mathbf{q}]\}$ is a Lie torus of type A_l, $l \geq 1$, and nullity n. It is shown in [9, Theorem 2.65] that every Lie torus of type A_l, $l \geq 3$, and nullity n is a central extension of $\mathfrak{sl}_{l+1}(F_\mathbf{q})$ for some quantum torus $F_\mathbf{q}$.

(d) Lie tori of type A_2 are classified in [9] and [10]. The centreless Lie tori of type A_1 are precisely the Tits-Kantor-Koecher algebras of the so-called Jordan tori, classified in [20]. A description of the centreless Lie tori is given in [4] for Δ of type $\mathrm{B}_l, \mathrm{C}_l, \mathrm{F}_4, \mathrm{G}_2$ and, under additional assumptions, in [5] for $\Delta = \mathrm{BC}_1$.

5. Theorem. *Let L be a Lie torus of type (Δ, Λ).*

(a) *L is finitely generated as Lie algebra, and has uniformly bounded dimension with respect to the $(\mathfrak{Q}(\Delta)\oplus\Lambda)$-grading (2.1), i.e., there exists a $M \in \mathbb{N}$ such that $\dim_F L_\alpha^\lambda \leq M$ for all $\alpha \in \Delta$ and $\lambda \in \Lambda$.*

(b) *The Lie algebra $\mathrm{Der}_F L$ of F-linear derivations of L is $(\mathfrak{Q}(\Delta)\oplus\Lambda)$-graded:*

$$\mathrm{Der}_F L = \bigoplus_{\alpha\in\Delta,\,\lambda\in\Lambda} (\mathrm{Der}_F L)_\alpha^\lambda , \tag{5.1}$$

where $(\mathrm{Der}_F L)_\alpha^\lambda$ consists of those derivations mapping L_β^μ to $L_{\alpha+\beta}^{\lambda+\mu}$. Moreover, $\mathrm{Der}_F L$ has uniformly bounded dimension with respect to the $(\mathfrak{Q}(\Delta)\oplus\Lambda)$-grading (5.1).

6. Let L be a Lie torus of type (Δ, Λ). Recall that the *centroid* of L, denoted $\mathrm{Cent}(L)$, is the set of all $\chi \in \mathrm{End}_F L$ satisfying $[\chi, \mathrm{ad}\, x] = 0$ for all $x \in L$. Since L is perfect, $\mathrm{Cent}(L)$ is a unital associative commutative algebra, and one can thus consider L as a module or as a Lie algebra over $\mathrm{Cent}(L)$. Since L is Δ-graded, a $\chi \in \mathrm{Cent}(L)$ leaves every root space L_α invariant. Moreover, χ is uniquely determined by $\chi|L_\alpha$ for a short root α. It follows that $\mathrm{Cent}(L)$ is Λ-graded, $\mathrm{Cent}(L) = \bigoplus_{\lambda\in\Lambda} \mathrm{Cent}(L)^\lambda$ with $\dim_F \mathrm{Cent}(L)^\lambda \leq 1$, where $\mathrm{Cent}(L)^\lambda$ consists of endomorphisms of degree λ with respect to the Λ-grading (3.1) of L. We put $\Gamma = \{\lambda \in \Lambda : \mathrm{Cent}(L)^\lambda \neq 0\}$. The following result justifies to call Γ the *centroid grading group.*

7. Theorem. *Let L be a centreless Lie torus of type (Δ, Λ).*

(a) *Γ is a subgroup of Λ, and $\mathrm{Cent}(L)$ is isomorphic to the group ring $F[\Gamma]$, hence to a Laurent polynomial ring in several variables.*

(b) *L is a free $\mathrm{Cent}(L)$-module. If $\Delta \neq \mathrm{A}_l$, then L has finite rank as $\mathrm{Cent}(L)$-module.*

Remarks. (a) Let $L = sl_{l+1}(F_\mathbf{q})$ as in Example 4.(c). In this case, $\mathrm{Cent}(L) = Z(F_\mathbf{q})\mathrm{Id}$, where $Z(F_\mathbf{q})$ denotes the centre of $F_\mathbf{q}$, and L has finite rank over $\mathrm{Cent}(L)$ if and only if $F_\mathbf{q}$ has finite rank over $Z(F_\mathbf{q})$, equivalently $[\Lambda : \Gamma] < \infty$. Using the description of $Z(F_\mathbf{q})$ given in [9, 2.44], it is easy to construct examples for which $\mathrm{rank}(\Gamma)$ takes on every value between 0 and n. In particular, L is in general not a finitely generated $\mathrm{Cent}(L)$-module.

(b) Let L be a centreless Lie torus. Then $\mathrm{Cent}(L)$ is an integral domain, acting without torsion on L. Let K be the quotient field of $\mathrm{Cent}(L)$, and let

$$\tilde{L} = L \otimes_{\mathrm{Cent}(L)} K \tag{7.1}$$

be its *central closure*, where in this tensor product L is considered as Lie algebra over $\mathrm{Cent}(L)$. Then L imbeds into $\tilde{L}$ and is a $\mathrm{Cent}(L)$-form of $\tilde{L}$. If L has finite rank over $\mathrm{Cent}(L)$, $\tilde{L}$ is a simple finite-dimensional Lie algebra over K.

8. Centroidal derivations. Let L be a centreless Lie torus of type (Δ, Λ), nullity n and centroidal grading group Γ. Recall the Λ-grading (3.1) of L. Any $\vartheta \in \mathrm{Hom}_{\mathbf{Z}}(\Lambda, F)$ induces a so-called *degree derivation* ∂_ϑ of L, defined by $\partial_\vartheta(x^\lambda) = \vartheta(\lambda)x^\lambda$ for $x^\lambda \in L^\lambda$. We put $\mathfrak{D} = \{\partial_\vartheta : \vartheta \in \mathrm{Hom}_{\mathbf{Z}}(\Lambda, F)\}$ and note that $\vartheta \mapsto \partial_\vartheta$ is an isomorphism from $\mathrm{Hom}_{\mathbf{Z}}(\Lambda, F)$ onto $\mathfrak{D}$, hence $\mathfrak{D} \cong F^n$. Moreover, $\mathfrak{D}$ induces the Λ-grading of L, i.e.,

$$L^\lambda = \{x \in L : \partial_\vartheta(x) = \vartheta(\lambda)x \text{ for all } \partial_\vartheta \in \mathfrak{D}\}. \tag{8.1}$$

If $\chi \in \mathrm{Cent}(L)$ then $\chi\partial \in \mathrm{Der}_F L$ for any $\partial \in \mathrm{Der}_F L$. It follows that $\mathrm{CDer}_F L = \mathrm{Cent}(L)\mathfrak{D} = \bigoplus_{\mu\in\Gamma} \mathrm{Cent}(L)^\mu\mathfrak{D}$ is a Γ-graded subalgebra of $\mathrm{Der}_F L$, called the algebra of *centroidal derivations of* L. It is a generalized Witt algebra in the sense of [18, 1.9].

9. Theorem. *Let L be a centreless Lie torus. Denote by* $\mathrm{IDer}L$ *the ideal of inner derivations of L. Then*

$$\mathrm{Der}_F L = \mathrm{IDer}L \rtimes \mathrm{CDer}_F L \quad \textit{(semidirect product)}. \tag{9.1}$$

In case L has finite rank as $\mathrm{Cent}(L)$-module, this result can be proven by using that its central closure $\tilde{L}$, see (7.1), is a finite-dimensional simple Lie K-algebra and hence all K-linear derivations are inner. In the remaining case, where L is a $\mathrm{Cent}(L)$-module of infinite rank, Δ is of type A by Theorem 7. Then the result follows from [9, 2.17, 2.53], [10, Theorem 1.40] and [18, Theorem 4.11]. For Δ of type B or D the splitting (9.1) has also been proven in [13, Corollary 4.9 and Corollary 4.10] using different methods. We note that the decomposition (9.1) is not the one proven in [6, Theorem 3.12] for arbitrary Δ-graded Lie algebras: the subalgebra $\mathrm{Der}_*(\mathfrak{a}, \mathfrak{S})$ of [6] contains $\mathrm{CDer}_F L$ but has in general a non-zero intersection with $\mathrm{IDer}L$.

References

1. B. Allison, S. Azam, S. Berman, Y. Gao, and A. Pianzola, *Extended affine Lie algebras and their root systems*, Mem. Amer. Math. Soc. **126** (1997), no. 603.
2. B. Allison, G. Benkart, and Y. Gao, *Lie algebras graded by the root systems BC_r, $r \geq 2$*, Mem. Amer. Math. Soc. **158** (2002), no. 751.
3. B. Allison, S. Berman, Y. Gao, and A. Pianzola, *A characterization of affine Kac-Moody Lie algebras*, Comm. Math. Phys. **185** (1997), 671–688.
4. B. Allison and Y. Gao, *The root system and the core of an extended affine Lie algebra*, Selecta Math. (N.S.) **7** (2001), 149–212.
5. B. Allison and Y. Yoshii, *Structurable tori and extended affine Lie algebras of type* BC_1, Pure Appl. Algebra **184** (2003), 105–138.
6. G. Benkart, *Derivations and invariant forms of Lie algebras graded by finite root systems*, Can. J. Math. **50** (1998), 225–241.
7. G. Benkart and O. Smirnov, *Lie algebras graded by the root system* BC_1, J. Lie Theory **13** (2003), 91–132.
8. G. Benkart and E. Zelmanov, *Lie algebras graded by finite root systems and intersection matrix algebras*, Invent. Math. **126** (1996), 1–45.

9. S. Berman, Y. Gao, and Y. Krylyuk, *Quantum tori and the structure of elliptic quasi-simple Lie algebras*, J. Funct. Anal. **135** (1996), 339–389.
10. S. Berman, Y. Gao, Y. Krylyuk, and E. Neher, *The alternative torus and the structure of elliptic quasi-simple Lie algebras of type A_2*, Trans. Amer. Math. Soc. **347** (1995), 4315–4363.
11. S. Berman and R. Moody, *Lie algebras graded by finite root systems and the intersection matrix algebras of Slodowy*, Invent. Math. **108** (1992), 323–347.
12. N. Bourbaki, *Éléments de mathématiques*, Groupes et Algèbres de Lie, Chapitres 4–6, Masson, Paris, 1981.
13. A. Duff, *Derivations of orthosymplectic Lie superalgebras*, Comm. Algebra **31** (2003), 2675–2705.
14. R. Moody, S. Eswara Rao, and T. Yokonuma, *Toroidal Lie algebras and vertex representations*, Geom. Dedicata **35** (1990), 283–307.
15. E. Neher, *Extended affine Lie algebras*, C. R. Math. Acad. Sci. Soc. R. Can. **26** (2004), 90–96.
16. E. Neher, *Lie algebras graded by 3-graded root systems and Jordan pairs covered by a grid*, Amer. J. Math **118** (1996), 439–491.
17. E. Neher, *An introduction to universal central extensions of Lie superalgebras*, in: Groups, rings, Lie and Hopf algebras (St. John's, NF, 2001), Math. Appl. **555**, 141–166. Kluwer Acad. Publ., Dordrecht, 2003.
18. E. Neher and Y. Yoshii, *Derivations and invariant forms of Jordan and alternative tori*, Trans. Amer. Math. Soc. **355** (2003), 1079–1108.
19. Y. Yoshii, *Lie tori – a simple characterization of extended affine Lie algebras*, Preprint 2003.
20. Y. Yoshii, *Coordinate algebras of extended affine Lie algebras of type A_1*, J. Algebra **234** (2000), 128–168.
21. Y. Yoshii, *Root-graded Lie algebras with compatible grading*, Comm. Algebra **29** (2001), 3365–3391.
22. Y. Yoshii, *Classification of division $\mathbf{Z}^n$-graded alternative algebras*, J. Algebra **256** (2002), 28–50.
23. Y. Yoshii, *Root systems extended by an abelian group and their Lie algebras*, (to appear in J. Lie Theory), 2003.

Department of Mathematics and Statistics
University of Ottawa
Ottawa, Ontario
K1N 6N5
email: neher@uottawa.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. 26, (3), 2004 pp. 90–96

EXTENDED AFFINE LIE ALGEBRAS

ERHARD NEHER

Presented by R. V. Moody, FRSC

RÉSUMÉ. On décrit une construction qui permet de construire tous les algèbres de Lie affines étendues à partir des tores de Lie.

ABSTRACT. We present a construction of all extended affine Lie algebras in terms of Lie tori.

0. Introduction. Extended affine Lie algebras are a class of complex Lie algebras that includes finite-dimensional simple Lie algebras, affine Lie algebras and toroidal Lie algebras. They are closely related to Saito's elliptic Lie algebras [13]. Originally proposed by the physicists Høegh-Krohn and B. Torrésani [8] under the name irreducible quasi-simple Lie algebras, extended affine Lie algebras have been put on a sound mathematical footing in the AMS-memoirs [1] by Allison, Azam, Berman, Gao and Pianzola. In particular, one can find there a detailed study of the root systems appearing in extended affine Lie algebras. The structure and representation theory of various classes of these Lie algebras has since been investigated in many papers. In this note we will describe the structure of extended affine Lie algebras in general.

Referring the reader to the main body of this note for precise definitions, we will only give a rough sketch of the relevant structures in this introduction. Two important properties of an extended affine Lie algebra are the existence of an invariant nondegenerate form and a finite-dimensional self-centralizing ad-diagonalizable subalgebra H. Thus E has a root space decomposition $E = \bigoplus E_\xi$ and a root system R, consisting of those $\xi \in H^*$ with $E_\xi \neq 0$. The form on E gives rise to a partition $R = R^0 \cup R^\times$ into isotropic roots R^0 and non-isotropic roots $R^\times$, generalizing the decomposition into imaginary and real roots in the affine case. Let E_c be the ideal generated by $\{E_\xi : \xi \in R^\times\}$, called the core of E. One assumes that E can be recovered from its core E_c in the sense that the kernel of the natural representation $E \to \mathrm{Der}E_c : x \mapsto \mathrm{ad}\, x|E_c$ lies in E_c. The core E_c may have a non-trivial centre, and it turns out to be easier to describe its central quotient $L = E_c/Z(E_c)$, where $Z(E_c)$ denotes the centre of E_c. The situation can thus be summarized by the following diagram

$$\begin{array}{ccc} E_c & \longrightarrow & E \\ \downarrow & & \\ L & & \end{array}$$

Received by the editors on March 5, 2004.
Partial support by a NSERC (Canada) discovery grant is gratefully acknowledged
AMS subject classification: Primary 17B65; Secondary 17B67, 17B70.

familiar from the affine case where E_c is the derived algebra and L a loop algebra. In general, the Lie algebras L appearing in (0.1) can be characterized without any reference to extended affine Lie algebras: they are Lie tori as defined in Yoshii's recent preprints [15] and [14] or in the preceding article [11]. Moreover, it is shown in [14] that all centreless Lie tori appear as the "bottom algebra" in a diagram (0.1). The canonical approach to untangling the structure of an extended affine Lie algebra E is therefore to describe (I) the centreless Lie tori L and (II) how to get from L to E.

Some results on (I) have been announced in the preceding article [11]. In this note we announce a solution of (II) in general (Theorem 6 and Theorem 8). Our construction, given in **5**, describes all extended affine Lie algebras with a given centreless core. It resembles the construction of affine Lie algebras and gives a new interpretation to certain subalgebras appearing in the previously known solution for the case $\Delta = \mathrm{A}_n$, $n \geq 2$. They are described here as subalgebras of skew centroidal derivations.

While the work on Lie tori can be done for Lie algebras over fields of characteristic 0, one has up to now only considered complex extended affine Lie algebras since one of their defining axioms is a topological (discreteness) condition. To remedy this discrepancy, we are proposing here a new definition of an extended affine Lie algebra over an arbitrary field F of characteristic 0. Roughly speaking, we are allowing more possibilities for the subalgebra $H \subset E$. In case $F = \mathbb{C}$ the algebras satisfying the old axiom system are recovered as the discrete extended affine Lie algebras in our sense (Theorem 8).

We continue with the terminology and notation of the preceding article [11].

1. A preliminary setting. Let E be a Lie algebra satisfying the following two axioms (EA1) and (EA2):

(EA1) E has a nondegenerate invariant symmetric bilinear form $(\ |\ )$.
(EA2) E contains a nontrivial finite-dimensional self-centralizing and ad-diagonalizable subalgebra H.

By (EA2), E has a root space decomposition $E = \bigoplus_{\xi \in H^*} E_\xi$ with $E_0 = H$, where, as usual, $E_\xi = \{e \in E : [h, e] = \xi(h)e \text{ for all } h \in H\}$. The invariance of $(\ |\ )$ implies that $(E_\xi | E_\zeta) = 0$ for $\xi + \zeta \neq 0$. It follows that $(\ |\ )$ restricted to $H \times H$ is nondegenerate. We can therefore transfer the restricted form $(\ |\ )|_{H \times H}$ to a nondegenerate symmetric bilinear form on H^* by setting $(\xi|\zeta) = (t_\xi | t_\zeta)$ where $t_\xi \in H$ is defined by $(t_\xi | h) = \xi(h)$ for all $h \in H$. We define

$$R = \{\xi \in H^* : E_\xi \neq 0\} \quad \text{(root system of } E\text{)},$$

$$R^0 = \{\xi \in R : (\xi|\xi) = 0\} \quad \text{(isotropic roots)},$$

$$R^\times = \{\xi \in R : (\xi|\xi) \neq 0\} \quad \text{(nonisotropic roots)}.$$

The subalgebra E_c of E, generated by $\{E_\xi : (\xi|\xi) \neq 0\}$ is called the *core of* E. It is in fact an ideal if E is an extended affine Lie algebra as defined below.

2. Definition. An *extended affine Lie algebra of nullity* n, or extended affine Lie algebra for short, is a Lie algebra E satisfying (EA1), (EA2) of **1** and, in addition, the following axioms (EA3)–(EA6):

(EA3) For $\xi \in R^\times$ and $x_\xi \in E_\xi$, the endomorphism $\operatorname{ad} x_\xi \in \operatorname{End}_F L$ is locally nilpotent.

(EA4) $R^\times$ is *irreducible*, i.e., $R^\times = R_1 \cup R_2$ and $(R_1|R_2) = 0$ implies $R_1 = \varnothing$ or $R_2 = \varnothing$.

(EA5) E is *tame* in the sense that $\{e \in E : [e, E_c] = 0\} \subset E_c$.

(EA6) $\Lambda := \langle R^0 \rangle \subset V$ is a free abelian group of rank n.

It is appropriate to immediately point out that this definition for $F = \mathbb{C}$ is more general than the usual definition of an extended affine Lie algebra ([1] or **7** below). The relation between the two definitions is discussed in **7** and **8**. As we will see, there is a close connection between extended affine Lie algebras and Lie tori. The following proposition is the first step in this direction. It can be proven using the techniques of [1, Ch. I] and [11, Thm. 5].

3. Proposition. *Let E be an extended affine Lie algebra with root system R, and put $\Lambda = \langle R^0 \rangle$.*

(a) *There exists a finite irreducible root system Δ, an imbedding $\Delta_{\text{ind}} \hookrightarrow R$ and a family $(\Lambda_\alpha : \alpha \in \Delta) \subset \Lambda$ such that*

$$V = \operatorname{span}_{\mathbb{Q}}(\Delta) \oplus \operatorname{span}_{\mathbb{Q}}(R^0) \quad \text{and} \quad R = \bigcup_{\alpha \in \Delta} (\alpha \oplus \Lambda_\alpha).$$

The subspaces $(E_c)^\lambda_\alpha = E_c \cap E_{\alpha \oplus \lambda}$ give E_c the structure of a Lie torus of type (Δ, Λ).

(b) *The root spaces E_ξ of E have uniformly bounded finite dimension.*

We note that the family $(\Lambda_\alpha : \alpha \in \Delta^\times)$ is a "reduced root system of type Δ extended by Λ" in the terminology of [15]. Theorem 2.4 of that paper gives the structure of this family, generalizing [1, II, Thm. 2.37].

4. Skew centroidal derivations. Let L be a centreless Lie torus. It follows from [14, Thm. 2.2 and Thm. 7.1] that L has a non-zero invariant (necessarily) symmetric bilinear form $(\ |\ )$, which is Λ-graded in the sense that $(L^\lambda | L^\mu) = 0$ if $\lambda + \mu \neq 0$. Moreover, any such form is unique up to a non-zero scalar, and is nondegenerate since L is centreless. In the following, we fix such a form $(\ |\ )$.

Recall the definition of the centroidal derivations in [11, §8]. Let $\operatorname{SCDer}_F L$ be the subalgebra of $\operatorname{CDer}_F L$ consisting of skew derivations with respect to the form $(\ |\ )$. Then $\operatorname{SCDer}_F L = \bigoplus_{\mu \in \Gamma} (\operatorname{SCDer}_F L)^\mu$ is Γ-graded with 0-component $\mathcal{D}$. One can show that $\operatorname{SCDer}_F L$ is the semidirect product of the subalgebra $\mathcal{D}$ of degree derivations and the ideal $\mathcal{D}' = \bigoplus_{0 \neq \mu \in \Gamma} (\operatorname{SCDer}_F L)^\mu$.

Proposition 3 associates a centreless Lie torus to every extended affine Lie algebra E, namely $L = E_c/Z(E_c)$. We will now describe a construction which, conversely, associates an extended affine Lie algebra to any centreless Lie torus.

5. Construction. Let L be a centreless Lie torus of type (Δ, Λ) and nullity n, and let $(\ |\ )$ be a nondegenerate invariant Λ-graded symmetric bilinear form on L. We denote by Γ the centroid grading group ([11, §6]).

The second ingredient of our construction is a Γ-graded subalgebra of $\mathrm{SCDer}_F L$,

$$D = \bigoplus_{\gamma\in\Gamma} D_\gamma, \quad D_\gamma \subset (\mathrm{SCDer}_F L)^\gamma,$$

which has the property that D_0 induces the Λ-grading [11, (3.1)] of L, i.e., $L^\lambda = \{x \in L : \partial_\theta(x) = \theta(\lambda)x \text{ for all } \partial_\theta \in D_0\}$. Equivalently, the canonical evaluation map

$$\mathrm{ev}\colon \Lambda \to D_0^* : \lambda \mapsto \mathrm{ev}(\lambda), \quad \text{where } \big(\mathrm{ev}(\lambda)\big)(\partial_\theta) = \theta(\lambda), \tag{5.1}$$

is injective. Let $D^{\mathrm{gr}*} = \bigoplus_{\gamma\in\Gamma} D_\gamma^*$ be the graded dual space of D. Thus, $f \in D_\gamma^*$ is extended to a linear form on D by $f|D_\delta = 0$ for $\delta \neq \gamma$. We consider $D^{\mathrm{gr}*}$ as a Γ-graded vector space with γ-component $(D^{\mathrm{gr}*})_\gamma = D^*_{-\gamma}$. It is easily seen that $\sigma_D\colon L\times L \to D^{\mathrm{gr}*}$, $\sigma_D(x,y)(d) = (dx|y)$ is a 2-cocycle for L with values in the trivial L-module $D^{\mathrm{gr}*}$ which respects the gradings of L and $D^{\mathrm{gr}*}$.

The third ingredient of our construction is a 2-cocycle $\tau\colon D\times D \to D^{\mathrm{gr}*}$ of D with values in $D^{\mathrm{gr}*}$, considered a D-module via the contragredient action $d\cdot f$, which is graded and invariant, i.e.,

$$\tau(D_\gamma, D_\delta) \subset (D^{\mathrm{gr}*})_{\gamma+\delta} = D^*_{-\gamma-\delta} \quad \text{and} \quad \tau(d_1,d_2)(d_3) = \tau(d_2,d_3)(d_1) \tag{5.2}$$

for $d_1, d_2, d_3 \in D$. Moreover, we suppose that

$$\tau(D_0, D) = 0. \tag{5.3}$$

Let $D' = \bigoplus_{0\neq\gamma\in\Gamma} D_\gamma$, an ideal of D. Because of condition (5.3), the map $\tau \mapsto \tau|D'\times D'$ is a bijection between the 2-cocycles of D satisfying (5.2) and (5.3) and the 2-cocycles of D' with values in the D'-module $D^{\mathrm{gr}*}$ satisfying (5.2).

Finally, for L, D and τ as above we define

$$E = E(L, D, \tau) = L \oplus D^{\mathrm{gr}*} \oplus D.$$

Then E is a Lie algebra with respect to the product ($x_i \in L, f_i \in D^{\mathrm{gr}*}, d_i \in D$)

$$\begin{aligned}[x_1 \oplus f_1 \oplus d_1\,,\, x_2 \oplus f_2 \oplus d_2] = {}& \big([x_1,x_2] + d_1(x_2) - d_2(x_1)\big)\\ & \oplus \big(\sigma_D(x_1,x_2) + d_1\cdot f_2 - d_2\cdot f_1 + \tau(d_1,d_2)\big) \oplus [d_1,d_2].\end{aligned}$$

Moreover, E has a nondegenerate invariant form $(\ |\ )$ given by

$$(x_1 \oplus f_1 \oplus d_1 | x_2 \oplus f_2 \oplus d_2) = (x_1|x_2) + f_1(d_2) + f_2(d_1).$$

Let $H = \mathfrak{h} \oplus D_0^* \oplus D_0$ for $\mathfrak{h}$ as in [11, (3.3)]. We identify $\Lambda = \mathrm{ev}(\Lambda) \subset D_0^*$ and view $\Lambda \subset H^*$ by letting $\lambda \in \Lambda$ act by 0 on $\mathfrak{h} \oplus D_0^*$. Similarly, any $\alpha \in \Delta \subset \mathfrak{h}^*$ gives rise to a linear form on H by putting $\alpha | D_0^* \oplus D_0 = 0$. With these identifications, H becomes a self-centralizing, ad-diagonalizable subalgebra of E whose root spaces are

$$E_{\alpha \oplus \lambda} = \begin{cases} L_\alpha^\lambda & ; \alpha \neq 0, \\ L_0^\lambda \oplus D_{-\lambda}^* \oplus D_\lambda & ; \alpha = 0. \end{cases}$$

It is then easy to verify part (a) of the following theorem.

6. Theorem. (a) *The algebra $E(L, D, \tau)$ constructed in* **5** *above is an extended affine Lie algebra of nullity n with respect to the form $(\ |\ )$ and the subalgebra H.*

(b) *Conversely, let E be an extended affine Lie algebra of nullity n and let $L = E_c/Z(E_c)$, which by Proposition* 3 *is a centreless Lie torus of nullity n. Then there exists a unique subalgebra $D \subset \mathrm{SCDer}_F L$ inducing the Λ-grading of L and a 2-cocycle $\tau\colon D \times D \to D^{\mathrm{gr}*}$ satisfying* (5.2) *and* (5.3) *such that $E \cong E(L, D, \tau)$.*

For the proof of part (b) we note that tameness of E and Proposition 3(b) imply that E can be described in terms of a Γ-graded subalgebra $D \subset \mathrm{Der}_F L$ with $D \cap \mathrm{IDer}_F L = 0$ and a 2-cocycle τ. Because of [11, Thm. 9] one can take $D \subset \mathrm{SCDer}_F L$.

Remarks. (a) The construction of the Lie algebra $E(L, D, \tau)$ makes sense in the more general setting where L is just a Lie algebra with a nondegenerate invariant form and D is a subalgebra of skew-symmetric derivations of L. For finite-dimensional algebras the Lie algebra $E(L, D, 0)$, called a *double extension*, has been used to classify finite-dimensional solvable Lie algebras admitting a nondegenerate invariant form ([8], [9, Ex. 2.10, 2.11], [10]). The more general construction with a possibly non-zero τ appears in [6, §3]. In the setting of discrete extended affine Lie algebras of type $\Delta = \mathrm{A}_l$, $l \geq 2$, the construction $E(L, D, \tau)$ appears in [4] and [5].

(b) Since $\mathrm{SCDer}_F L$ induces the Λ-grading of L, $D = \mathrm{SCDer}_F L$ is the maximal choice for D. In this case the subalgebra $L \oplus (\mathrm{SCDer}_F L)^*$ of E is the universal central extension of L. As pointed out in [4, Remark 3.71(b)], there do indeed exist non-trivial 2-cocycles τ in this case, which first have appeared in the context of toroidal Lie algebras ([12], see also [3, (2.11), (2.12)]).

7. Definition. Let E be a Lie algebra over $F = \mathbb{C}$. We call E a *discrete extended affine Lie algebra* if E satisfies the axioms (EA1)–(EA5) and the following axiom

(DE) R is a discrete subset of H^*.

In view of [2, Lemma 3.62] a discrete extended affine Lie algebra as defined above is the same as a tame extended affine Lie algebra in the sense of [1]. We have included tameness in our definition, i.e., the axiom (EA5), since our results apply to tame extended affine Lie algebras only. Moreover, as an example in [4, §3] shows, there is little hope to get a precise description of extended affine Lie algebras that are not tame. Besides the mentioned example in [4], all of the known constructions yield tame extended affine Lie algebras.

8. Theorem. *Let $F = \mathbb{C}$.* (a) *Let L be a centreless Lie torus and let D be a graded subalgebra of* $\mathrm{SCDer}_{\mathbb{C}}L$ *such that the evaluation map* $\mathrm{ev}\colon \Lambda \to D_0^*$ *of* (5.1) *is not only injective but has also discrete image. Then, with τ as in the construction* **5**, *the Lie algebra $E(L, D, \tau)$ is a discrete extended affine Lie algebra.*

(b) *Conversely, every discrete extended affine Lie algebra arises from the construction described in* (a).

We note that $\mathrm{ev}\colon \Lambda \to \mathfrak{D}^*$ is always a discrete imbedding. Hence any complex Lie torus gives rise to a discrete extended affine Lie algebra ([14, Cor. 7.3]). A construction of discrete imbeddings in terms of the maximal choice $D = \mathfrak{D}$ is given in [7, §2] (although not in this language).

References

1. B. Allison, S. Azam, S. Berman, Y. Gao, and A. Pianzola, *Extended affine Lie algebras and their root systems*, Mem. Amer. Math. Soc. **126** (1997), no. 603.
2. B. Allison, S. Berman, and A. Pianzola, *Covering algebras. I. Extended affine Lie algebras*, J. Algebra, **250** (2002), 485–516.
3. S. Berman and Y. Billig, *Irreducible representations for toroidal Lie algebras*, J. Algebra, **221** (1999), 188–231.
4. S. Berman, Y. Gao, and Y. Krylyuk, *Quantum tori and the structure of elliptic quasi-simple Lie algebras*, J. Funct. Anal., **135** (1996), 339–389.
5. S. Berman, Y. Gao, Y. Krylyuk, and E. Neher, *The alternative torus and the structure of elliptic quasi-simple Lie algebras of type A_2*, Trans. Amer. Math. Soc., **347** (1995), 4315–4363.
6. M. Bordemann, *Nondegenerate invariant bilinear forms on nonassociative algebras*, Acta Math. Univ. Comenian. (N.S.), **66** (1997), 151–201.
7. Y. Gao, *The degeneracy of extended affine Lie algebras*, Manuscripta Math., **97** (1998), 233–249.
8. K. Hofmann and V. Keith, *Invariant quadratic forms on finite-dimensional Lie algebras*, Bull. Austral. Math. Soc., **33** (1986), 21–36.
9. V. Kac, *Infinite-dimensional Lie algebras*, Cambridge University Press, Cambridge, third edition, 1990.
10. A. Medina and P. Revoy, *Algèbres de Lie et produit scalaire invariant*, Ann. Sci. École Norm. Sup. (4), **18** (1985), 553–561.

11. E. Neher, *Lie tori*, C. R. Math. Acad. Sci. Soc. R. Can. **26** (2004), 84–89.
12. S. Eswara Rao and R. Moody. *Vertex representations for n-toroidal Lie algebras and a generalization of the Virasoro algebra*, Comm. Math. Phys., **159** (1994), 239–264.
13. K. Saito and D. Yoshii, *Extended affine root system. IV. Simply-laced elliptic Lie algebras*, Publ. Res. Inst. Math. Sci., **36** (2000), 385–421.
14. Y. Yoshii, *Lie tori – a simple characterization of extended affine Lie algebras*. Preprint 2003.
15. Y. Yoshii, *Root systems extended by an abelian group and their Lie algebras*, J. Lie Theory, to appear.

Department of Mathematics and Statistics
University of Ottawa,
Ottawa, Ontario
K1N 6N5
email: neher@uottawa.ca