On Bhargava's representations and Vinberg's invariant theory

Benedict H. Gross*
Department of Mathematics, Harvard University
Cambridge, MA 02138
gross@math.harvard.edu

January, 2011

1 Introduction

Manjul Bhargava has recently made a great advance in the arithmetic theory of elliptic curves. Together with his student, Arul Shankar, he determines the average order of the Selmer group $\mathbf{Sel}(E, m)$ for an elliptic curve E over $\mathbf{Q}$, when $m = 2, 3, 4, 5$. We recall that the Selmer group is a finite subgroup of $H^1(\mathbf{Q}, E[m])$, which is defined by local conditions. Their result (cf. [1, 2]) is that the average order of $\mathbf{Sel}(E, m)$ is $\sigma(m) =$ (the sum of the divisors d of m) in these four cases (where $\sigma(m) = 3, 4, 7, 6$ respectively). Since the Selmer group contains the subgroup $E(\mathbf{Q})/mE(\mathbf{Q})$, they are able to conclude that the average rank of elliptic curves over $\mathbf{Q}$ is bounded above by a constant which is less than 1. We expect that the average rank is equal to $1/2$, although this is the first result which proves that the average rank is bounded!

Their calculation, which involves some beautiful geometry of numbers, requires an explicit description of the stable orbits in four integral representations:

$\mathbf{SL}_2/\mu_2$ on $\mathrm{Sym}^4(\mathbb{Z}^2)$ for m = 2,

$\mathbf{SL}_3/\mu_3$ on $\mathrm{Sym}^3(\mathbb{Z}^3)$ for m = 3,

$(\mathbf{SL}_2 \times \mathbf{SL}_4)/\mu_4$ on $\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^4)$ for m = 4,

$(\mathbf{SL}_5 \times \mathbf{SL}_5)/\mu_5$ on $\mathbb{Z}^5 \otimes \wedge^2(\mathbb{Z}^5)$ for m = 5.

In their work, these representations appear naturally when one considers principal homogenous spaces for the m-torsion subgroup of E. In the case $m = 2$, the representation and its polynomial invariants

*Supported by NSF grant DMS-0901102

were initially investigated by Hermite (cf. [9]).

In this note we will show how all four of these representations also arise (over the complex numbers) in Vinberg's invariant theory, applied to specific automorphims of finite order $m = 2, 3, 4, 5$ of the exceptional simple groups $\mathbf{G} = \mathbf{G}_2, \mathbf{F}_4, \mathbf{E}_7, \mathbf{E}_8$. We then discuss a generalization of the case $m = 2$, to the Selmer groups of the Jacobians of hyper-elliptic curves with a rational Weierstrass point.

2 Distinguished maximal parabolic subgroups

Let $\mathbf{G}$ be a complex reductive group, and let $\lambda : \mathbf{GL}_1 \to \mathbf{G}$ be an injective homomorphism. Associated to λ we have:

1. the Levi subgroup $\mathbf{L}$ of $\mathbf{G}$ which centralizes the image, and
2. a $\mathbb{Z}$-grading of $\mathfrak{g} = \bigoplus \mathfrak{g}(a)$ of the Lie algebra $\mathfrak{g}$ of $\mathbf{G}$.

The grading is by the eigenspaces of the induced $\mathbf{GL}_1$ action: for an integer a the subspace $\mathfrak{g}(a)$ is where $\lambda(t)$ acts by multiplication by t^a. Then $\mathfrak{g}(0)$ is the Lie algebra of $\mathbf{L}$ and $\bigoplus_{a \geq 0} \mathfrak{g}(a)$ is the Lie algebra of a parabolic subgroup $\mathbf{P}$ with Levi subgroup $\mathbf{L}$.

The exceptional groups $\mathbf{G}_2, \mathbf{F}_4, \mathbf{E}_8$ each have a unique distinguished maximal parabolic subgroup, up to conjugacy [4]. This corresponds to a unique $\mathbf{G}$-conjugacy class of $\lambda : \mathbf{GL}_1 \to \mathbf{G}$ which satisfies the two conditions

1. the centralizer of $\mathbf{L}$ in $\mathbf{G}$ is equal to $\lambda(\mathbf{GL}_1)$,
2. $\dim(\mathfrak{g}(1)) = \dim(\mathfrak{g}(0))$.

The only other simple group which has a distinguished maximal parabolic subgroup, or equivalently, which has a homomorphism λ satisfying these two conditions, is $\mathbf{G} = \mathbf{PGL}_2$, where $\mathbf{P}$ is a Borel subgroup and $\mathbf{L}$ is a maximal torus. In these four examples, the Levi subgroup $\mathbf{L}$ has a dense open orbit on the representation $\mathfrak{g}(1)$, with a finite stabilizer. When $\mathbf{G} = \mathbf{PGL}_2$, the stabilizer is trivial. In the three exceptional cases, the stabilizer is isomorphic to the finite symmetric group $\mathbf{S}_3, \mathbf{S}_4, \mathbf{S}_5$ respectively.

Let $\mathbf{T}$ be a maximal torus in $\mathbf{G}$ which contains the image of λ. Since the parabolic subgroup $\mathbf{P}$ is maximal, the co-character $\lambda : \mathbf{GL}_1 \to \mathbf{T}$ is a fundamental co-weight for $\mathbf{T}$. We tabulate the Levi subgroup $\mathbf{L}$ and the representations $\mathfrak{g}(a)$ of $\mathbf{L}$ below. Since $\mathfrak{g}(0)$ is the Lie algebra of $\mathbf{L}$, and $\mathfrak{g}(-a)$ is dual to $\mathfrak{g}(a)$ under the Killing form, we will only tabulate the representations $\mathfrak{g}(a)$ for $a \geq 1$. They were calculated from the table of roots in [3].

$\mathbf{G}$	$\mathbf{L}$	$\mathfrak{g}(a)$	dim
$\mathbf{G}_2$	$(\mathbf{GL}_1 \times \mathbf{SL}_2)/\mu_2$	$\mathfrak{g}(1) = \lambda \otimes \mathrm{Sym}^3(2)$ $\mathfrak{g}(2) = \lambda^2 \otimes 1$	4 1
$\mathbf{F}_4$	$(\mathbf{GL}_1 \times \mathbf{SL}_2 \times \mathbf{SL}_3)/\mu_6$	$\mathfrak{g}(1) = \lambda \otimes 2 \otimes \mathrm{Sym}^2(3)$ $\mathfrak{g}(2) = \lambda^2 \otimes 1 \otimes \mathrm{Sym}^2(3)^*$ $\mathfrak{g}(3) = \lambda^3 \otimes 2 \otimes 1$	12 6 2
$\mathbf{E}_8$	$(\mathbf{GL}_1 \times \mathbf{SL}_4 \times \mathbf{SL}_5)/\mu_{20}$	$\mathfrak{g}(1) = \lambda \otimes 4 \otimes \wedge^2(5)$ $\mathfrak{g}(2) = \lambda^2 \otimes \wedge^2(4) \otimes \wedge^4(5)$ $\mathfrak{g}(3) = \lambda^3 \otimes \wedge^3(4) \otimes 5$ $\mathfrak{g}(4) = \lambda^4 \otimes 1 \otimes \wedge^3(5)$ $\mathfrak{g}(5) = \lambda^5 \otimes 4 \otimes 1$	40 30 20 10 4

When $\mathbf{G}$ is the complex adjoint group of type $\mathbf{E}_7$, there are no distinguished maximal parabolic subgroups. However, there is a fundamental co-weight λ which has $\dim \mathfrak{g}(0) = 27$ and $\dim \mathfrak{g}(1) = 24$. In this case, there is an open orbit of $\mathbf{L}$ on $\mathfrak{g}(1)$ with stabilizer isogenous to $\mathbf{SL}_2$. Here is a table of the analogous information.

$\mathbf{E}_7$	$(\mathbf{GL}_1 \times \mathbf{SL}_2 \times \mathbf{SL}_3 \times \mathbf{SL}_4)/\mu_2 \times \mu_{12}$	$\mathfrak{g}(1) = \lambda \otimes 2 \otimes 3 \otimes 4$ $\mathfrak{g}(2) = \lambda^2 \otimes 1 \otimes \wedge^2(3) \otimes \wedge^2(4)$ $\mathfrak{g}(3) = \lambda^3 \otimes 2 \otimes 1 \otimes \wedge^3(4)$ $\mathfrak{g}(4) = \lambda^4 \otimes 1 \otimes 3 \otimes 1$	24 18 8 3

3 Vinberg's invariant theory

We obtain a $(\mathbb{Z}/m\mathbb{Z})$ grading of the Lie algebra $\mathfrak{g}$, for $\mathbf{G} = \mathbf{G}_2, \mathbf{F}_4, \mathbf{E}_7, \mathbf{E}_8$, by restricting the homomorphism $\lambda : \mathbf{GL}_1 \to \mathbf{G}$ to the finite subgroup μ_m of $\mathbf{GL}_1$, for $m = 2, 3, 4, 5$ respectively.

Let $\mathbf{G}(0)$ be the centralizer of the finite subgroup $\lambda(\mu_m)$ in $\mathbf{G}$. This reductive group contains the Levi subgroup $\mathbf{L}$ tabulated above, and has Lie algebra the sum of the three eigenspaces $\mathfrak{g}(-m)+\mathfrak{g}(0)+\mathfrak{g}(m)$. Let V be the representation of $\mathbf{G}(0)$ on the sum of the two eigenspaces $\mathfrak{g}(1)+\mathfrak{g}(1-m)$. This is precisely the subspace of $\mathfrak{g}$ where each ζ in μ_m acts by multiplication by ζ. Vinberg studies the representation of $\mathbf{G}(0)$ on the eigenspace V for a general torsion automorphism of $\mathbf{G}$, and shows that it has a polynomial ring of invariants. (For Vinberg's original papers see [6, 7, 8]; for an excellent survey of this work see [5].)

From the tabulation of the individual representations $\mathfrak{g}(a)$, we find the following groups and representations.

m	$\mathbf{G}$	$\mathbf{G}(0)$	V	dim
2	$\mathbf{G}_2$	$(\mathbf{SL}_2 \times \mathbf{SL}_2)/\mu_2$	$2 \otimes \mathrm{Sym}^3(2)$	8
3	$\mathbf{F}_4$	$(\mathbf{SL}_3 \times \mathbf{SL}_3)/\mu_3$	$3 \otimes \mathrm{Sym}^2(3)$	18
4	$\mathbf{E}_7$	$(\mathbf{SL}_2 \times \mathbf{SL}_4 \times \mathbf{SL}_4)/\mu_2 \times \mu_4$	$2 \otimes 4 \otimes 4$	32
5	$\mathbf{E}_8$	$(\mathbf{SL}_5 \times \mathbf{SL}_5)/\mu_5$	$5 \otimes \wedge^2(5)$	50

The last case is one of the four representations considered by Bhargava. In the first three cases, when $m = 2, 3, 4$, the finite subgroup $\lambda(\mu_m)$ normalizes a simply-connected subgroup $\mathbf{H}$ of $\mathbf{G}$, of type $\mathbf{A}_2, \mathbf{D}_4, \mathbf{E}_6$ respectively, and induces an (outer) automorphism of order m of $\mathbf{H}$. We obtain a smaller representation of the subgroup $\mathbf{H}(0)$ on the corresponding eigenspace V_H of the Lie algebra $\mathfrak{h}$ of $\mathbf{H}$.

m	$\mathbf{H}$	$\mathbf{H}(0)$	V_H	dim
2	${}^2\mathbf{A}_2$	$(\mathbf{SL}_2)/\mu_2$	$\mathrm{Sym}^4(2)$	5
3	${}^3\mathbf{D}_4$	$(\mathbf{SL}_3)/\mu_3$	$\mathrm{Sym}^3(3)$	10
4	${}^2\mathbf{E}_6$	$(\mathbf{SL}_2 \times \mathbf{SL}_4)/\mu_4$	$2 \otimes \mathrm{Sym}^2(4)$	20

These three cases, together with the case $m = 5$ above, are the four representations considered by Bhargava in his study of the m-Selmer group.

4 The complex reflection group

In Vinberg's theory, each of the four representations V_H constructed above has a two dimensional Cartan subspace $\mathfrak{c}$ of semi-simple commuting elements in $\mathfrak{h}$, which is unique up to conjugation by $\mathbf{H}(0)$. The subgroup of $\mathbf{H}(0)$ which stabilizes $\mathfrak{c}$ is finite, and lies in an exact sequence (with $m = 2, 3, 4, 5$)

$$1 \longrightarrow (\mathbb{Z}/m\mathbb{Z})^2 \longrightarrow Stab(\mathfrak{c}) \longrightarrow W_m \longrightarrow 1.$$

Moreover, the group W_m is a finite complex reflection group, which embeds as a discrete subgroup of $\mathbf{U}(2)$. It has the presentation

$$W_m = \{s, t : s^m = t^m = 1, sts = tst\}.$$

We note that when $m \geq 6$ this presentation yields an infinite group. For $m = 6$, W_m is the rotation subgroup of the affine Weyl group of type $\mathbf{G}_2$, and for $m \geq 7$, W_m embeds as a discrete subgroup of $\mathbf{U}(1, 1)$.

For $m \leq 5$, the $\mathbf{H}(0)$-invariant polynomials on V_H restrict isomorphically to the W_m-invariant polynomials on the Cartan subspace $\mathfrak{c}$. These invariants form a polynomial ring with two generators I and J in the degrees tabulated below.

m	$degrees$	W_m	$Card(W_m)$
2	$2, 3$	$S_3 = \mathbf{SL}_2(\mathbb{Z}/2\mathbb{Z})$	6
3	$4, 6$	$2.A_4 = \mathbf{SL}_2(\mathbb{Z}/3\mathbb{Z})$	24
4	$8, 12$	$4.S_4 = 2 \times \mathbf{SL}_2(\mathbb{Z}/4\mathbb{Z})$	96
5	$20, 30$	$10.A_5 = 5 \times \mathbf{SL}_2(\mathbb{Z}/5\mathbb{Z})$	600

The restriction of the discriminant from $\mathfrak{h}$ to V_H has the form Δ^{m-1}, where Δ is an invariant polynomial of degree $6, 12, 24, 60$ on V_H. We have $\Delta = -4.I^3 - 27.J^2$ in the usual normalization. The orbits of $H(0)$ where $\Delta \neq 0$ are closed and have finite stabilizers, so are stable in the sense of geometric invariant theory. Associated to such an orbit, we have the elliptic curve E with equation

$$y^2 = x^3 + I.x + J$$

and the stabilizer of any vector in the orbit is the m-torsion subgroup $E[m] = (\mathbb{Z}/m\mathbb{Z})^2$.

5 Hyperelliptic curves with a Weierstrass point

The case $m = 2$ considered above has the following generalization in Vinberg's theory. Assume that $n \geq 1$ and let θ be the pinned outer involution of $\mathbf{H} = \mathbf{PGL}_{2n+1} = \mathbf{PGL}(W)$. Then $\mathbf{H}(0)$ is the special orthogonal group $\mathbf{SO}(W)$ and the eigenspace $V_H = \mathfrak{h}(1)$ affords the irreducible representation $\mathrm{Sym}^2(W)_0$ of dimension $(2n^2 + 3n)$ of $\mathbf{H}(0) = \mathbf{SO}(W)$. A Cartan subspace $\mathfrak{c}$ of V_H has dimension $2n$, and the stabilizer of $\mathfrak{c}$ is a finite subgroup of $\mathbf{SO}(W)$, which lies in the exact sequence

$$1 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{2n} \longrightarrow Stab(\mathfrak{c}) \longrightarrow S_{2n+1} \longrightarrow 1.$$

In this case, the invariant polynomials on V_H have degrees $2, 3, ..., 2n + 1$. If we view $\mathfrak{h} = \mathfrak{sl}_{2n+1}$ as the Lie algebra of endomorphisms of trace zero of W, then $\mathfrak{h}(1)$ is the subspace of self-adjoint endomorphisms $T = T^*$ of trace zero. The $\mathbf{H}(0)$- invariant polynomials are generated by the coefficients of the characteristic polynomial of T:

$$F(x) = x^{2n+1} + I_2 x^{2n-1} + I_3 x^{2n-2} + ... + I_{2n+1}.$$

In this case, $\Delta(T) = \Delta(I_2, I_3, ...I_{2n+1})$ is the discriminant of the characteristic polynomial.

The orbits with $\Delta(T) \neq 0$ are stable. Associated to such an orbit we have the hyperelliptic curve of genus n with affine equation $y^2 = F(x)$ having a fixed Weierstrass point above $x = \infty$. The stabilizer of any vector in the orbit is the 2-torsion subgroup $J[2]$ of the Jacobian J. Using this description of the stable orbits and some geometry of numbers, Bhargava and I hope to prove that the average order of the 2-Selmer group $\mathbf{Sel}(J, 2)$ for this family of hyperelliptic curves over $\mathbf{Q}$ is equal to 3.

References

[1] M. Bhargava, A. Shankar *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, ArXiv: 1006.1002 (2010).

[2] M. Bhargava, A. Shankar *Ternary cubic forms having bounded invariants and the existence of a positive proportion of elliptic curves having rank* 0 ArXiv: 1007.0052 (2010).

[3] N. Bourbaki *Groupes et algèbres de Lie* Hermann (1982).

[4] R. Carter *Finite groups of Lie type* Wiley (1985).

[5] D. Panyushev *On invariant theory of θ-groups* J. Algebra **283** (2005), pp. 655-670.

[6] E.B. Vinberg *On the linear groups associated to periodic automorphims of semi-simple Lie algebras.* Soviet Math Dokl. **16** (1975), pp. 406-409.

[7] E.B. Vinberg *On the classification of the nilpotent elements of graded Lie algebras.* Soviet Math Dokl. **16** (1975), pp. 1517-1520.

[8] E.B. Vinberg *The Weyl group of a graded Lie algebra* Mathematics of the USSR, Izvestija **10** (1976), pp. 463-495.

[9] A. Weil *Remarques sur un mémoire d'Hermite* Arch. Math **5** (1954), pp. 197-202.