SMITH NORMAL FORM AND LAPLACIANS

DINO LORENZINI

Abstract. Let M denote the Laplacian matrix of a graph G. Associated with G is a finite group $\Phi(G)$, obtained from the Smith normal form of M, and whose order is the number of spanning trees of G. We provide some general results on the relationship between the eigenvalues of M and the structure of $\Phi(G)$, and address the question of how often the group $\Phi(G)$ is cyclic.

1. Introduction

Let G be a connected graph with $n > 1$ vertices $v_1, \ldots, v_n$ and m edges (adjacent vertices may be linked by more than one edge). Let A denote its adjacency matrix. Let d_i denote the degree of v_i, and set $D := \mathrm{diag}(d_1, \ldots, d_n)$, the diagonal matrix of the degrees. Let $M := D - A$, the Laplacian matrix of G.

This article considers a circle of problems related to the finitely generated abelian group $\mathbb{Z}^n/\mathrm{Im}(M)$. This group can be computed in practice using the Smith normal form of M, as follows. Given any $(n \times n)$-invertible integer matrices P and Q and any $(n \times n)$-integer matrix N with $PNQ = \mathrm{diag}(s_1, \ldots, s_n)$, it is easy to show that $\mathbb{Z}^n/\mathrm{Im}(N)$ is isomorphic to $\prod_{i=1}^n \mathbb{Z}/s_i\mathbb{Z}$. In our case, the rank of M is $n-1$, with kernel generated by the transpose of the vector $(1, \ldots, 1)$. If M is row and column equivalent over the integers to $\mathrm{diag}(s_1, \ldots, s_{n-1}, 0)$, then $\mathbb{Z}^n/\mathrm{Im}(M) \cong \prod_{i=1}^{n-1} \mathbb{Z}/s_i\mathbb{Z} \times \mathbb{Z}$. A canonical diagonal matrix equivalent to a given matrix N is obtained as follows: let $\Delta_r := \Delta_r(N)$ denote the greatest common divisor of the determinants of all $(r \times r)$-minors of N. The matrix N is row and column equivalent to $\mathrm{diag}(\Delta_1, \Delta_2/\Delta_1, \ldots, \Delta_n/\Delta_{n-1})$.

Denote by $\Phi(G)$ the torsion part of this group, so that $\Phi(G)$ is a finite abelian group, and $\mathbb{Z}^n/\mathrm{Im}(M)$ is isomorphic to $\mathbb{Z} \times \Phi(G)$. The order of $\Phi(G)$ is $\Delta_{n-1}(M)$, and this integer is a well-known graph invariant, the *number $\kappa(G)$ of spanning trees* of G, also called the *complexity* of G. We have thus a factorization of $\kappa(G)$ given by $\Delta_1 \cdot \Delta_2/\Delta_1 \cdot \ldots \cdot \Delta_{n-1}/\Delta_{n-2}$. It is natural to wonder what properties of a graph are reflected in this factorization.

Maybe the earliest result in the literature concerning this factorization is a result of Berman ([4] (1986), page 7, prop. 4.1), which states that the factorizations of the complexities of a planar graph and its dual are identical. This result was rediscovered in [15], and in [3] Prop. 8, and generalized in [26].

The group $\Phi(G)$ occurs in the literature under at least four different names, depending on the context in which it is used. It may have first appeared in the literature in 1970 in [34], 8.1.2, page 64, in the context of arithmetic geometry. This material can now also found be in the main reference text for the subject, [9], 9.6.

(a) In 1989, motivated by problems in arithmetic geometry, the author initiated a purely graph theoretical study of $\Phi(G)$ in [28], where the group $\Phi(G)$ is called the *group of components*, in keeping with the terminology used in arithmetic geometry.
(b) In 1990, Dhar considered this group in the context of physics in [19], where the group is called the *sandpile group*.

Date: February 22, 2008.

(c) In 1997, motivated by the theory of algebraic curves, Bacher at al. considered $\Phi(G)$ in [3], where $\Phi(G)$ is called the *Picard group*, shown to be isomorphic to a group called the *jacobian group*.
(d) In 1999, Biggs studied chip firing games in [6], where the group $\Phi(G)$ is called the *critical group*.
(e) In 1990, the analogous group associated with the Smith normal form of the adjacency matrix A of G is called *Smith group* in [35].

The group $\Phi(G)$ can obviously be generated by at most $n-1$ generators, and also by at most $\beta(G) := m - n + 1$ generators ([28], p. 281). If a graph G is obtained from a graph G_0 by adding a single edge, then the minimal number of generators of the groups $\Phi(G)$ and $\Phi(G_0)$ can differ by at most 1 ([27], 5.2). If a graph G is obtained from two graphs G' and G'' by gluing one vertex of G' to a vertex of G'', then $\Phi(G) = \Phi(G') \times \Phi(G'')$. Little else is known in general on the minimal number of generators of $\Phi(G)$, and on how the structure of the group $\Phi(G)$ reflects the combinatorial properties of G.

There is a very large body of knowledge regarding the Laplacian eigenvalues of a graph. It is thus natural, when searching for relationships between the structure of $\Phi(G)$ and the combinatorial properties of the graph, to start by understanding first the relationships between the eigenvalues of M and its Smith normal form. This general study is done in the next section of this article. The eigenvalues of M do contribute to the structure of the group $\Phi(G)$, but they do not determine it. In the third section, we completely determine the structure of the group $\Phi(G)$ when G is a conference graph on n vertices, with n squarefree.

The explicit determination of the structure of $\Phi(G)$ in a given family of graphs is not always easy, and one finds in the literature in the last ten years a series of papers whose goal is to explicitly determine the structure of classes of groups $\Phi(G)$. For instance, examples of families containing exactly one graph on n vertices for each integer n are found in [6], [7], [17], and [23]. Larger families are studied in [14], [24], and [38].

We say that G is *cyclic* when the group $\Phi(G)$ is cyclic. When considering very 'symmetric' graphs, one often finds that the associated group $\Phi(G)$ is not cyclic. On the other hand, if one randomly picks a graph G and computes its group $\Phi(G)$, should one expect that G is often cyclic? In other words, should one expect that $\Delta_{n-2}(M) = 1$ often, where M is the Laplacian of G? Obviously, this question as phrased is rather vague, and we discuss various rigorous density notions of cyclic graphs in section 4.

In the fifth section, we study one family of graphs where the proportion of cyclic groups, when counted appropriately, is at least $6/\pi^2$. In the last section of this article, we introduce a simple criterion (6.5) for a graph G to have a cyclic group $\Phi(G)$, and we show that for many graphs G with $\Phi(G)$ cyclic, this criterion can be used to produce infinitely many non-isomorphic other graphs with cyclic groups.

I thank Grant Fiddyment for computations in 3.4, for the data in 4.3, and for the example in 6.4; thanks also to Brandon Samples and Nathan Walters for computations in 3.3 and 3.4, to Andrew Granville for the proof of 4.10, to G. Michael Guy for sharing his Maple scripts and computations for 5.5 and 5.12, and to the participants in the Graph Seminar at the University of Georgia for helpful comments. I would also like to thank the referee for helpful comments and corrections.

2. Eigenvalues and Smith Normal form

We study in this section the relationships between the eigenvalues and the Smith normal form of the Laplacian of a graph, and, more generally, of any integer $(n \times n)$-matrix M

of rank $n-1$. In the more general context of any integer matrix M, this question is considered in [33] and [36]. In the special case of the adjacency matrix of a graph G, this question is considered in [35].

Let $n>1$ be an integer, and let M be any $(n\times n)$-integer matrix of rank $n-1$. Let $\Phi(M)$ denote the torsion subgroup of $\mathbb{Z}^n/\mathrm{Im}(M)$. As we shall see, when $\lambda=0$ is a simple eigenvalue of M, the other eigenvalues are indeed related to the order of the group $\Phi(M)$, but they do not in general determine the structure of $\Phi(M)$.

Let R denote an integer vector generating the kernel of M. Write the transpose of R as $(r_1,\ldots,r_n)$, and assume that $\gcd(r_1,\ldots,r_n)=1$. Let R' be the corresponding vector for the transpose ${}^tM$ of M, and write ${}^tR'=(r'_1,\ldots,r'_n)$, with $\gcd(r'_1,\ldots,r'_n)=1$. Let $r:=R\cdot R'$ denote the dot product of R and R'. We always choose R and R' such that $r\geq 0$. An example where $r=0$ is given in 2.15. When M is symmetric, we always choose $R'=R$. When M is the Laplacian of a graph, ${}^tR=(1,\ldots,1)$ and $R\cdot R=n$. Let M^* denote the *comatrix* of M (also called the *adjoint matrix* of M): the matrix M^* has coefficient in row i and column j equal to $(-1)^{i+j}$ times the determinant of the minor of M obtained by removing row j and column i from M. We have $MM^*=M^*M=\det(M)\mathrm{Id}_n$.

Let G be a connected graph, and let $\lambda_1\geq\cdots\geq\lambda_{n-1}$ denote the non-zero eigenvalues of its Laplacian M. Our first proposition generalizes the well-known relation between the spectrum of M and the complexity of G (see, e.g., [21], 13.2.4):

$$\lambda_1\cdot\ldots\cdot\lambda_{n-1}=n\kappa(G). \tag{1}$$

Proposition 2.1. *Let M be any $(n\times n)$-integer matrix of rank $n-1$, with characteristic polynomial $\mathrm{char}_M(x)=x\prod_{i=1}^{n-1}(x-\lambda_i)$. Then $M^*=\pm|\Phi(M)|R\,({}^tR')$, and*

$$\prod_{i=1}^{n-1}\lambda_i=\pm|\Phi(M)|(R'\cdot R).$$

In particular, $\lambda=0$ is a simple root of $\mathrm{char}_M(x)$ if and only if $(R'\cdot R)\neq 0$.

If $(R'\cdot R)=0$, then M is not diagonalizable. When M is diagonalizable, $(R'\cdot R)$ divides the product of the distinct non-zero eigenvalues of M.

Proof. Since $MM^*=0$, we find that each column vector of M^* is an integer multiple of R. Thus there exists an integer vector A whose transpose ${}^tA=(a_1,\ldots,a_n)$ is such that $M^*=R(a_1,\ldots,a_n)$. Similarly, from $M^*M=0$, there exists an integer vector B whose transpose $(b_1,\ldots,b_n)$ is such that $M^*=B({}^tR')$. Clearly, since M has rank $n-1$, the vectors R,R',A, and B, are all not zero. Pick an index i such that $r'_i\neq 0$. Then $a_iR=r'_iB$. It follows that $a_i\neq 0$. Since $\gcd(r_1,\ldots,r_n)=1$, we conclude that $r'_i\mid a_i$, so that $B=cR$ for some integer $c\neq 0$. Similarly, we find that $A=dR'$ for some $d\neq 0$. It follows that $c=d$ and $M^*=cR({}^tR')$. The coefficients of M^* are the determinants of the $(n-1)$-minors of M. Since the coefficients of R and R' are coprime, we conclude that c is up to a sign the greatest common divisor of the $(n-1)$-minors of M. In other words, since $\det(M)=0$, we find that $c=\pm|\Phi(M)|$.

Consider the relation $M\prod_{i=1}^{n-1}(M-\lambda_i\mathrm{Id}_n)=0$. Let $N:=\prod_{i=1}^{n-1}(M-\lambda_i\mathrm{Id}_n)$. The same argument as above shows that there exists an integer a such that $N=aR({}^tR')$. Thus, $NR=((-1)^{n-1}\prod_{i=1}^{n-1}\lambda_i)R=arR$. Since the coordinates of R are coprime, $(-1)^{n-1}\prod_{i=1}^{n-1}\lambda_i=ar$. To show that $a=\pm|\Phi(M)|$, we recall that the coefficient of x in the characteristic polynomial of any matrix can be computed as the sum of the determinants of the principal $(n-1)$-minors of M. In our case, using our description of M^*, we find that this sum is $\pm|\Phi(M)|(\sum_{i=1}^n r_ir'_i)=\pm|\Phi(M)|(R\cdot R')$, as desired.

Assume that M is diagonalizable. Let $\lambda_1, \ldots, \lambda_t$ denote the distinct non-zero eigenvalues of M. Then $M\prod_{i=1}^{t}(M-\lambda_i \mathrm{Id}_n) = 0$. As before, we find that $\prod_{i=1}^{t}(M-\lambda_i \mathrm{Id}_n) = bR({}^tR')$ for some non-zero integer b. Thus, $\pm(\prod_{i=1}^{t}\lambda_i)R = b(R\cdot R')R \neq 0$, and $(R\cdot R') \neq 0$. □

2.2 Since the order of $\Phi(M)$ is so obviously related to the eigenvalues of M when $r > 0$, it is natural to wonder whether it is possible to construct explicit non-trivial elements of $\Phi(M)$ using eigenvectors of M. We do so first for integer eigenvalues.

Let $w := (w_1, \ldots, w_n) \in \mathbb{Z}^n$ be an eigenvector of M for a non-zero integer eigenvalue λ. Then the class of w in $\Phi(M)$ has order dividing λ. Indeed, $Mw = \lambda w$ shows that $\lambda w \in \mathrm{Im}(M)$. It may happen however that the class of w is trivial in $\Phi(M)$, even when $\gcd(w_1, \ldots, w_n) = 1$. For instance, when $G = K_n$, $f_1 = (1, -1, 0, \ldots, 0)$, $f_2 = (1, 0, -1, \ldots, 0)$, $\ldots$, and $f_{n-1} = (1, 0, \ldots, 0, -1)$, are $n-1$ linearly independent eigenvectors for the eigenvalue n. Clearly, $w := \sum f_i$ is also an eigenvector for n, but $w \in \mathrm{Im}(M)$.

Let $\mathrm{ord}_p(x)$ denote the largest power of a prime p that divides the integer x.

Proposition 2.3. *Let M be any $(n\times n)$-integer matrix of rank $n-1$ as above, with $r > 0$. Let $\lambda \neq \pm 1$ be a non-zero integer eigenvalue of multiplicity $m(\lambda)$. Let $\mu(\lambda)$ denote the maximal number of linearly independent eigenvectors for the eigenvalue λ.*

(1) *Let w be an integer eigenvector of M for λ. Assume that the greatest common divisor of its coefficients is 1. Then the order of the class of w in $\Phi(M)$ is divisible by $\lambda/\gcd(\lambda, r)$ and divides λ (2.2). Let w' be any integer eigenvector of ${}^tM$ for λ, with $w\cdot w' \neq 0$. Then the order of the class of w in $\Phi(M)$ is divisible by $\lambda/\gcd(\lambda, w\cdot w')$.*
(2) *If there exists a prime p such that $p \mid \lambda$ but $p \nmid r$, then $\Phi(M)$ contains a subgroup isomorphic to $(\mathbb{Z}/p^{\mathrm{ord}_p(\lambda)}\mathbb{Z})^{\mu(\lambda)}$.*
(3) *If M is symmetric and the vector R has one entry r_i with $r_i = \pm 1$, then $\Phi(M)$ contains a subgroup isomorphic to $(\mathbb{Z}/\lambda\mathbb{Z})^{\mu(\lambda)-1}$.*

Proof. (1) We know from 2.2 that the order c of the class of w in $\Phi(M)$ divides λ. Thus there exists an integer vector u such that $Mu = cw$ and, hence, $M((\lambda/c)u - w) = 0$. We can thus find an integer d such that $(\lambda/c)u - w = dR$. If $d = 0$, then λ/c divides each coefficient of w, so $c = \lambda$. Assume now that $d \neq 0$. Taking the dot product of the latter equality with the vector R' shows that

$$(\lambda/c)(u\cdot R') = dr.$$

It follows that $\frac{\lambda}{c\gcd(\lambda/c, r)}$ divides d. Since $w = (\lambda/c)u - dR$ has all its coefficients divisible by $\frac{\lambda}{c\gcd(\lambda/c,r)}$, we find that $\lambda/c = \gcd(\lambda/c, r)$, so that $\lambda/c \mid r$. It follows that $\lambda/\gcd(\lambda, r)$ divides c.

Since ${}^tw'MR = 0 = \lambda w'\cdot R$, we conclude that $w'\cdot R = 0$. Assume that $d > 0$. From $(\lambda/c)u - w = dR$, we obtain that $(\lambda/c)(u\cdot w') = (w\cdot w')$. Thus, $\lambda/\gcd(\lambda, w\cdot w')$ divides $c\frac{w\cdot w'}{\gcd(\lambda, w\cdot w')}$, and c is divisible by $\lambda/\gcd(\lambda, w\cdot w')$.

(2) Let $V_\lambda \subseteq \mathbb{Z}^n$ denote the $\mathbb{Z}$-submodule generated by the set of eigenvectors in $\mathbb{Z}^n$ for the eigenvalue $\lambda \in \mathbb{Z}$. Consider a basis $w^{(1)}, \ldots, w^{(\mu(\lambda))}$ for the $\mathbb{Z}$-module $V_\lambda \subseteq \mathbb{Z}^n$. Note that the submodule V_λ is saturated, that is, if $v \in \mathbb{Z}^n$ and $tv \in V_\lambda$ for some integer t, then $v \in V_\lambda$.

Suppose that there exist integers a_i and an integer vector u such that $Mu = \sum a_i w^{(i)}$. Then we can find an integer d such that $\lambda u - \sum a_i w^{(i)} = dR$. Taking the dot product of this expression with R', we find that $\lambda/\gcd(\lambda, r)$ divides d. Since $\sum a_i w^{(i)} = \lambda u - dR = (\lambda/\gcd(\lambda, r))w'$ with $w' \in V_\lambda$, we can find integers b_i such that $\sum a_i w^{(i)} = (\lambda/\gcd(\lambda, r))\sum b_i w^{(i)}$. It follows that $\lambda/\gcd(\lambda, r)$ divides a_i for all $i = 1, \ldots, \mu(\lambda)$.

Let p^e denote the exact power of p dividing λ. Part (1) implies that the class of $w^{(i)}$ has order divisible by $\lambda/\gcd(\lambda, r)$. By assumption, $p \nmid r$. Let then $v^{(i)} := g_i w^{(i)}$ denote the smallest multiple of $w^{(i)}$ whose order in $\Phi(M)$ is p^e. Our hypothesis implies that $p \nmid g_i$ for all i. Suppose that $\sum d_i(\text{class of } v^{(i)}) = 0$ in $\Phi(M)$. Then there exists an integer vector u such that $Mu = \sum d_i v^{(i)}$. The above discussion shows that $\lambda/\gcd(\lambda, r)$ divides $d_i g_i$ for all i. Then $p^e \mid d_i$ for all i, and we find that $\Phi(M)$ contains a subgroup isomorphic to $(\mathbb{Z}/p^e\mathbb{Z})^{\mu(\lambda)}$.

(3) Without loss of generality, we may assume that $r_1 = \pm 1$. Adding (or subtracting) all rows to the first row and all columns to the first column shows that the group $\Phi(M)$ is isomorphic to the group $\Phi(M^{(1,1)})$. The minor $M^{(1,1)}$ is nonsingular, and thus we can use [36], Theorem 4, to show that $\Phi(M^{(1,1)})$ contains a subgroup isomorphic to $(\mathbb{Z}/\lambda\mathbb{Z})^\nu$ if $M^{(1,1)}$ has ν linearly independent eigenvectors for the eigenvalue λ.

Recall (see, e.g., [21], 9.1) that if $\lambda_1 \geq \cdots \geq \lambda_n$ denote the eigenvalues of M, and $\theta_1 \geq \cdots \geq \theta_{n-1}$ denote the eigenvalues of $M^{(1,1)}$, then

$$\lambda_1 \geq \theta_1 \geq \lambda_2 \geq \cdots \geq \theta_{n-1} \geq \lambda_n.$$

Thus, if λ is an eigenvalue for M with multiplicity $m(\lambda)$, then it is also an eigenvalue for $M^{(1,1)}$ with multiplicity at least $m(\lambda) - 1$. □

Remark 2.4 The statement (3) is meaningful when $\mu(\lambda) > 1$. When M is not symmetric, the weaker condition $m(\lambda) > 1$ is not sufficient, as the following example shows. Let

$$M := \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

The transposes of R and R' are $(1, -\lambda, \lambda^2)$ and $(0, 0, 1)$, respectively. Hence, $r = \lambda^2$. The eigenvalue λ clearly has multiplicity 2. It is easy to check that $\Phi(M)$ is trivial, so that $\Phi(M)$ does not have an element of order λ.

Remark 2.5 Let G be a connected graph on n vertices without multiple edges. Let G^c denote the complement of G in K_n, assumed to be connected. If $\lambda_1 \geq \cdots \geq \lambda_{n-1} > 0$ are the eigenvalues of G, then the eigenvalues of G^c are $n - \lambda_{n-1} \geq \cdots \geq n - \lambda_1 \geq 0$ ([21], 13.1.3). In particular, an eigenvalue λ for G and the eigenvalue $n - \lambda$ for G^c have same multiplicity, $m(\lambda)$.

Suppose now that G has an integer eigenvalue $1 < \lambda < n-1$ coprime to n, of multiplicity $m(\lambda) > 1$. Then both $\Phi(G)$ and $\Phi(G^c)$ cannot be generated by fewer than $m(\lambda)$ elements. Indeed, 2.3 implies it directly for $\Phi(G)$. Under our hypotheses, $n - \lambda > 1$ and is coprime to n, so we may apply 2.3 to obtain that $\Phi(G^c)$ cannot be generated by fewer than $m(\lambda)$ elements.

The group $\Phi(G)$ is completely described in [14] for a large class of graphs G having only integer (Laplacian) eigenvalues. Conjecture 7 in [14] would imply that for threshold graphs G with an integer eigenvalue $n > \lambda > 0$ of multiplicity $m(\lambda)$, then $\Phi(G)$ always contains a subgroup isomorphic to $(\mathbb{Z}/\lambda\mathbb{Z})^{m(\lambda)}$, even when $\lambda \mid n$ (see [14], Example 14).

Conjecture 7 in [14] also implies for threshold graphs G that each summand of $\Phi(G)$ has order a product of distinct eigenvalues of G, so that $\Phi(G)$ is killed by the product of the distinct eigenvalues of G. This latter fact follows for all graphs from our next proposition, which generalizes [36], Theorem 2.

Proposition 2.6. *Let $M \neq 0$ be a diagonalizable $(n \times n)$-integer matrix. Let $\lambda_1, \ldots, \lambda_t$ denote the distinct non-zero eigenvalues of M. Let $\Phi(M)$ denote the torsion subgroup of $\mathbb{Z}^n/\mathrm{Im}(M)$. Then $\Phi(M)$ is killed by $\prod_{i=1}^t \lambda_i$.*

Proof. Let K denote the splitting field of the characteristic polynomial of M. Let $\mathcal{O}_K$ denote its ring of integers. Since M has integer coefficients, each λ_i is an algebraic integer, and the product $\prod_{i=1}^t \lambda_i$ is an integer.

Consider the natural map $(\mathbb{Z}^n/M(\mathbb{Z}^n))_{\mathrm{tors}} \to (\mathcal{O}_K^n/M(\mathcal{O}_K^n))_{\mathrm{tors}}$. This map is injective. Indeed, if $v \in \mathbb{Z}^n$ can be written $Mw = v$ with $w \in \mathcal{O}_K^n$, write $PMQ = D$ with P, Q, and D integer matrices, and P, Q invertible, D diagonal. The relation $DQ^{-1}w = Pv$ shows that all coefficients of $Q^{-1}w$ belong to $\mathbb{Q}$, except possibly for $(n - \mathrm{rank}(M))$ of them, say the $(n - \mathrm{rank}(M))$ last ones. The first $\mathrm{rank}(M)$ coefficients of $Q^{-1}w$ are then integral and rational, so they are integers. Let u denote the vector $Q^{-1}w$ where its last $(n - \mathrm{rank}(M))$ coefficients have been replaced by 0. Then u has integer coefficients, and $Du = Pv$. Thus $MQu = v$, with $Qu \in \mathbb{Z}^n$, so that the class of v is trivial in $(\mathbb{Z}^n/M(\mathbb{Z}^n))_{\mathrm{tors}}$.

We are going to show that $\prod_{i=1}^t \lambda_i$ kills the (additive) group $(\mathcal{O}_K^n/M(\mathcal{O}_K^n))_{\mathrm{tors}}$. Let $v_0 \in (\mathcal{O}_K^n/M(\mathcal{O}_K^n))_{\mathrm{tors}}$. Choose a vector $v \in \mathcal{O}_K^n$ representing v_0. Then there exist $v_i \in K^n$, $i = 1, \ldots, t$, such that $v = \sum_{i=1}^t v_i$, and for each $i = 1, \ldots, t$, v_i is an eigenvector for λ_i. Indeed, by assumption there exists $d \in \mathbb{N}$ such that $dv \in \mathrm{Im}(M)$, and $\mathrm{Im}(M)$ is generated over K by the eigenvectors for the non-zero eigenvalues. Let $w := \sum_{i=1}^t v_i/\lambda_i$. We have $Mw = v$ by construction. We claim that $u := (\prod_{i=1}^t \lambda_i)w$ is a vector with integral coefficients. Once this claim is proved, it follows from $Mu = (\prod_{i=1}^t \lambda_i)v$ that v has order dividing $(\prod_{i=1}^t \lambda_i)$ in $\mathcal{O}_K^n/M(\mathcal{O}_K^n)$, as desired.

We use as in [36] an induction on the number of distinct non-zero vectors v_i appearing in the representation $v = \sum v_i$. If $v = v_1$, then $\lambda_1(v_1/\lambda_1) = v$ is integral by hypothesis. Assume that now $v = \sum_{i=1}^k v_i$ for some $k > 1$. Then $Mv = \sum_{i=1}^k \lambda_i v_i$, and we apply the induction hypothesis to $Mv - \lambda_k v = \sum_{i=1}^{k-1} (\lambda_i - \lambda_k)v_i$, which belongs to $\mathcal{O}_K^n$. Therefore, the vector

$$\begin{aligned} (\textstyle\prod_{i=1}^{k-1} \lambda_i)(\sum_{i=1}^{k-1} \frac{\lambda_i - \lambda_k}{\lambda_i} v_i) &= (\textstyle\prod_{i=1}^{k-1} \lambda_i)(\sum_{i=1}^{k} v_i) - (\prod_{i=1}^{k} \lambda_i)(\sum_{i=1}^{k} v_i/\lambda_i) \\ &= (\textstyle\prod_{i=1}^{k-1} \lambda_i)v - (\prod_{i=1}^{k} \lambda_i)w \end{aligned}$$

is integral, and the result follows. □

Remark 2.7 When M is of rank $n - 1$, we showed in 2.1 that the product $\prod_{i=1}^t \lambda_i$ of the distinct eigenvalues is divisible by $R' \cdot R$. It is natural to wonder whether $\Phi(M)$ may be killed by $(\prod_{i=1}^t \lambda_i)/(R \cdot R')$. The answer to this question is negative, as shown by the bipartite graphs $K_{a,a}$, whose eigenvalues are 0, a, and $2a$, but $\Phi(K_{a,a}) = (\mathbb{Z}/a\mathbb{Z})^{2a-4} \times \mathbb{Z}/a^2\mathbb{Z}$.

If λ is an algebraic number, we let $N(\lambda)$, the *norm* of λ, denote the product of the roots of the minimal polynomial of λ over $\mathbb{Q}$.

Corollary 2.8. (a) *Assume that G is a graph with $\Phi(G)$ cyclic. Then an eigenvalue λ of G with $N(\lambda) \nmid n$ has multiplicity 1. If λ is an integer with $\lambda > 1$ and $\lambda \mid n$, then $m(\lambda) \leq 2$.*

(b) *Assume that G is a tree. Then all eigenvalues λ of G with $N(\lambda) \neq 1$ have $m(\lambda) = 1$.*

Proof. Let $\lambda_1, \ldots, \lambda_t$ denote the distinct non-zero eigenvalues of M, and let $m(\lambda_i)$ denote the multiplicity of λ_i. The group $\Phi(G)$ has order $\frac{1}{n} \prod_{i=1}^t \lambda_i^{m(\lambda_i)}$. If it is cyclic, we find that $\frac{1}{n} \prod_{i=1}^t \lambda_i^{m(\lambda_i)}$ divides $\prod_{i=1}^t \lambda_i$. If $m(\lambda) > 1$, either $N(\lambda) = 1$, or $N(\lambda) > 1$ and $N(\lambda) \mid n$. In the latter case, when λ is an integer, 2.3 (3) shows that $m(\lambda) - 1 \leq 1$.

Assume that G is a tree. Then $\prod_{i=1}^{t} \lambda_i^{m(\lambda_i)} = n$ and $n \mid \prod_{i=1}^{t} \lambda_i$ (2.1). It follows that if $m(\lambda) > 1$, then $N(\lambda) = 1$. □

Remark 2.9 The converse of the above corollary is not true, that is, $\Phi(G)$ not cyclic does not necessarily imply that some eigenvalue not dividing n has multiplicity greater than 1. Indeed, consider the graph G with adjacency matrix

$$\begin{pmatrix} 0 & 2 & 6 \\ 2 & 0 & 8 \\ 6 & 8 & 0 \end{pmatrix}.$$

Then $\Phi(G) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/38\mathbb{Z}$, and the characteristic polynomial of the Laplacian is $t(t^2 - 32t + 228)$, with three eigenvalues of multiplicity 1.

The cycle on n vertices is an example of a graph with $\Phi(G)$ cyclic, and eigenvalues of multiplicity 2. When G is a tree and $\lambda > 1$ is an integer, it is shown in [22], Theorem 2.1, that $m(\lambda) = 1$. An example of a tree with an eigenvalue $\lambda \notin \mathbb{Z}$, of multiplicity 2, and with $N(\lambda) = 1$, is found in [22], 3.5.

When λ is an eigenvalue of M which is not an integer, no eigenvector associated to λ is in $\mathbb{Z}^n$. Thus, the contribution of λ and its eigenvectors to the group $\Phi(M)$ is more subtle than in the case where $\lambda \in \mathbb{Z}$. To discuss it, we introduce the following integer.

Recall that an eigenvalue of M is always an algebraic integer, since it is the root of a monic polynomial with integer coefficients, the characteristic polynomial of M. Let λ be any algebraic integer with minimal monic polynomial $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Z}[x]$. Define the integer $L(\lambda)$, the *least common multiple of the roots* of the minimal polynomial of λ over $\mathbb{Q}$, to be the smallest positive integer L such that L/λ is an algebraic integer. This integer is the denominator of $1/\lambda$ in [2]. It follows that since both $L(\lambda)/\lambda$ and $N(\lambda)/\lambda$ are algebraic integers, so is $\gcd(L, N)/\lambda$. Hence, $L(\lambda) \mid N(\lambda)$. We give below a criterion for determining when $L(\lambda) = N(\lambda)$.

Lemma 2.10. *Let $f(x) = x^d + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Let λ be a root of $f(x)$.*

(1) *$L(\lambda)$ is the smallest positive integer L such that $a_i L^i/a_0 \in \mathbb{Z}$ for all $i = 1, \ldots, d$. In particular, $\frac{N(\lambda)}{L(\lambda)} \mid a_1$, and $N(\lambda) \mid L(\lambda)^d$.*

(2) *$L(\lambda) = N(\lambda)$ if and only if, for each prime p such that $p \mid \gcd(a_0, a_1)$, $\mathrm{ord}_p(a_0) = 1$.*

Proof. (1) Note that $\mathbb{Q}(\lambda) = \mathbb{Q}(L(\lambda)/\lambda)$, so that the minimal polynomial over $\mathbb{Q}$ of $L(\lambda)/\lambda$ has degree d. The polynomial $x^d f(L(\lambda)/x)/a_0$ has rational coefficients and has $L(\lambda)/\lambda$ as a root. It is thus the minimal polynomial of $L(\lambda)/\lambda$. Since we assume $L(\lambda)/\lambda$ to be an algebraic integer, $x^d f(L(\lambda)/x)/a_0 \in \mathbb{Z}[x]$. Thus, we find that $L(\lambda)$ is the smallest positive integer L such that $a_i L^i/a_0 \in \mathbb{Z}$ for all $i = 1, \ldots, d$. The cases where $i = 1$ and $i = d$ give (using $|a_0| = N(\lambda)$) that $\frac{N(\lambda)}{L(\lambda)} \mid a_1$, and $N(\lambda) \mid L(\lambda)^d$.

We can rewrite the above conditions as

$$\frac{a_0}{\gcd(a_0, a_i)} \mid L^i, \text{ for all } i = 1, \ldots, d.$$

Letting $\lceil y \rceil$ denote the smallest integer larger than y, we find that

$$\mathrm{ord}_p(L(\lambda)) = \max_j \left(\left\lceil \frac{\mathrm{ord}_p(a_0) - \mathrm{ord}_p(\gcd(a_0, a_j))}{j} \right\rceil \right).$$

(2) Since $L := L(\lambda)$ divides $N := N(\lambda)$ and $N \mid L^d$, we find that L and N are divisible by the same primes. Recall that N/L divides a_1. Then, if $p \nmid a_1$, $\mathrm{ord}_p(a_0) = \mathrm{ord}_p(N) = \mathrm{ord}_p(L)$. Suppose that $p \mid \gcd(a_0, a_1)$ and $\mathrm{ord}_p(a_0) = 1$. Since $p \mid a_0$, $p \mid L$. Since $L \mid N$, we must have $\mathrm{ord}_p(a_0) = \mathrm{ord}_p(N) = \mathrm{ord}_p(L) = 1$.

Suppose now that $L = N$. In particular, for each prime p, $\mathrm{ord}_p(L) = \mathrm{ord}_p(a_0)$. Let k denote an index such that $\mathrm{ord}_p(L(\lambda)) = \lceil \frac{\mathrm{ord}_p(a_0) - \mathrm{ord}_p(\gcd(a_0,a_k))}{k} \rceil$. If $k = 1$, we find that $p \nmid a_1$. In particular, when $p \mid a_1$, we have $k > 1$. We claim that if $k > 1$ and $\lceil \frac{a-b}{k} \rceil = a$ for some integers $0 \leq b \leq a$, then $a = 0$ or 1. Indeed, there exists $0 \leq \epsilon < 1$ such that $\lceil \frac{a-b}{k} \rceil = \frac{a-b}{k} + \epsilon$. Hence, $k\lceil \frac{a-b}{k} \rceil = (a-b) + k\epsilon = ka$. It follows that $k\epsilon - b = (k-1)a$. Since $k > 1$, $a \leq k\epsilon/(k-1) < 2$. Thus, $a = 0$ or 1. It follows that when $p \mid \gcd(a_0, a_1)$, $\mathrm{ord}_p(a_0) = 1$. □

Proposition 2.11. *Let M be an integer $(n \times n)$-matrix of rank $n-1$. Assume that $r > 0$. Let λ be an eigenvalue of M.*

(1) *Then $\Phi(M)$ contains an element of order $L(\lambda)/\gcd(L(\lambda), r)$.*
(2) *Assume that M is symmetric, and that the vector R has a coefficient r_i with $r_1 = \pm 1$. If the multiplicity of λ is greater than 1, then $\Phi(M)$ contains an element of order $L(\lambda)$.*

Proof. (1) Let $s_1 \mid \cdots \mid s_{n-1}$ denote the non-zero invariant factors of M ($s_i \in \mathbb{N}$, for all i) so that M has Smith normal form $\mathrm{diag}(s_1, \ldots, s_{n-1}, 0)$. Let $\lambda_1, \ldots, \lambda_{n-1}$ denote the non-zero eigenvalues of M (in any ordering, possibly with repetitions). Recall (2.1) that $\prod_{i=1}^{n-1} \lambda_i = \pm|\Phi(M)|r$. Theorem 6 in [33] states that there exists an algebraic integer c such that $c\prod_{i=1}^{n-2} s_i = \prod_{i=1}^{n-2} \lambda_i$. It follows that

$$\prod_{i=1}^{n-1} \lambda_i = (c\prod_{i=1}^{n-2} s_i)\lambda_{n-1} = \pm r(\prod_{i=1}^{n-1} s_i).$$

Hence, $c\lambda_{n-1} = \pm r s_{n-1}$. In other words, $r s_{n-1}/\lambda$ is an algebraic integer for any non-zero eigenvalue λ of M. Therefore, $L(\lambda) \mid r s_{n-1}$, and $\frac{L(\lambda)}{\gcd(L(\lambda),r)} \mid s_{n-1}$. Since s_{n-1} is the exponent of the abelian group $\Phi(M)$, there exists an element in $\Phi(M)$ of any order dividing s_{n-1}.

(2) We proceed as in the proof of 2.3 (3). Without loss of generality, we may assume that $r_1 = \pm 1$. Adding (or subtracting) all rows to the first row and all columns to the first column shows that the group $\Phi(M)$ is isomorphic to the group $\Phi(M^{(1,1)})$. The minor $M^{(1,1)}$ is nonsingular, and thus we can use [36], Theorem 1, to show that $\Phi(M^{(1,1)})$ contains an element of order $L(\lambda)$ if $M^{(1,1)}$ has eigenvalue λ. This latter fact is true if $m(\lambda) > 1$, and is proved in 2.3 (3). □

It is natural to wonder, in view of 2.3, (2) and (3), whether Part (2) of Proposition 2.11 can be sharpened (see for instance 3.7).

Example 2.12 Consider the symmetric matrix

$$M_a := \begin{pmatrix} a & 4 & 1 & 10 & 3 \\ 4 & 4 & 1 & 1 & 3 \\ 1 & 1 & 0 & 0 & 1 \\ 10 & 1 & 0 & 0 & 1 \\ 3 & 3 & 1 & 1 & 2 \end{pmatrix}.$$

The reader can verify that ${}^tR = (0, 1, -1, 0, -1)$, $r = 3$, and

$$\begin{array}{lcll} \mathrm{char}_{M_1}(t) & = & t(t^4 - 7t^3 - 125t^2 + 453t + 243), & L(\lambda) = 81, \quad \Phi(M_1) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}; \\ \mathrm{char}_{M_4}(t) & = & t(t^4 - 10t^3 - 107t^2 + 468t + 243), & L(\lambda) = 27, \quad \Phi(M_4) = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}; \\ \mathrm{char}_{M_5}(t) & = & t(t^4 - 11t^3 - 101t^2 + 473t + 243), & L(\lambda) = 243, \quad \Phi(M_5) = \mathbb{Z}/81\mathbb{Z}. \end{array}$$

All three polynomials of degree 4 above are irreducible over $\mathbb{Z}$.

It is also possible to exhibit graphs without multiple edges whose Laplacian M has a characteristic polynomial $xf(x)$ with $f(x)$ irreducible, $L(\lambda) < N(\lambda)$, and $\Phi(G)$ *not* cyclic.

Consider for instance a graph H on 8 vertices $\{1,2,3,4,5,6,7,8\}$ obtained as follows. Start with a cycle on 8 vertices, with edges $\{(1,2),(2,3),(3,4),(4,5),(5,6),(6,7),(7,8),(8,1)\}$, and add to it the edges $\{(1,3),(1,4),(4,6),(4,7)\}$. The group $\Phi(H)$ is cyclic. Consider now the complement G of H in K_8. The Laplacian of G has characteristic polynomial $t(t^7-32t^6+428t^5-3094t^4+13015t^3-31722t^2+41223t-21816)$, with the factor of degree 7 irreducible over $\mathbb{Z}$, and the group $\Phi(G)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/909\mathbb{Z}$.

Let Φ be an abelian group. It is well known that if $|\Phi|$ is squarefree, then Φ is cyclic. In particular, let M be an integer $(n\times n)$-matrix of rank $n-1$ with $r>0$. Write $\mathrm{char}_M(x) = xf(x)$, with $f(x) = x^{n-1}+\cdots+a_1x+a_0$. Then, if a_0/r is squarefree, then $\Phi(M)$ is cyclic. This latter statement is slightly generalized in our next lemma, with a hypothesis reminiscent of 2.10, (2).

Lemma 2.13. *Let M be an integer $(n\times n)$-matrix of rank $n-1$ with $r>0$. Write $\mathrm{char}_M(x) = xf(x)$, with $f(x) = x^{n-1}+\cdots+a_1x+a_0$. Assume that for each prime p with $p \mid \gcd(a_0,a_1)$, $\mathrm{ord}_p(a_0/r) = 1$. Then $\Phi(M)$ is cyclic.*

Proof. The coefficient a_1, which is the coefficient of x^2 in the characteristic polynomial of the matrix M, is, up to a sign, equal to the sum of the determinants of the principal $(n-2)\times(n-2)$-minors of M (see, e.g., [21], top of page 284). Suppose that $\Phi(M)$ is not cyclic. Then $\Delta_{n-2}(M)/\Delta_{n-3}(M) > 1$. Hence, there exists a prime number p dividing $\Delta_{n-2}(M) > 1$. Therefore, $p \mid a_1$ or $a_1 = 0$. Since $\Delta_{n-2}(M)/\Delta_{n-3}(M)$ divides $\Delta_{n-1}(M)/\Delta_{n-2}(M)$, we find that p^2 divides $\Delta_{n-1}(M) = a_0/r$. □

The proof of Proposition 2.11 only asserts the existence of an element of $\Phi(M)$ of order $L(\lambda)/\gcd(L(\lambda),r)$, but does not exhibit such an element. In our next lemma, we provide an instance where some precise information can be given about the order of a specific element in $\Phi(M)$ related to λ.

Let $K := \mathbb{Q}(\lambda)$, and denote by $\mathcal{O}_K$ its ring of integers. Let H denote the set of $[K:\mathbb{Q}]$ distinct embeddings $\sigma : K \to \mathbb{C}$. For any eigenvector $w \in \mathcal{O}_K^n$ for λ, the vector $t(w) := \sum_{\sigma\in H}\sigma(w)$ has integer coefficients, and $\sum_{\sigma\in H}\sigma(\frac{w}{\lambda})$ has rational coefficients. Let $u(w) := L(\lambda)\sum_{\sigma\in H}\sigma(\frac{w}{\lambda})$. This latter vector has coefficients in $\mathbb{Q}\cap\mathcal{O}_K = \mathbb{Z}$. Consider the relation

$$Mu(w) = L(\lambda)\ t(w).$$

Since both $t(w)$ and $u(w)$ are integer vectors, this relation shows that the class of $t(w)$ in $\Phi(M)$ has order dividing $L(\lambda)$.

When the vector w had integer coefficients, we used in an essential way in the proof of 2.3 that the greatest common divisor of the coefficients of w was 1. When $\mathcal{O}_K$ is not a principal ideal domain, the analogue property is not available, and we need to proceed as follows. Let p be a prime number, and let $\mathbb{Z}_{(p)}$ denote the localization of $\mathbb{Z}$ at the ideal (p). The integral closure of $\mathbb{Z}_{(p)}$ in K is the ring of fractions $B := T^{-1}\mathcal{O}_K$, where $T := \mathbb{Z}\setminus\{(p)\}$ ([30], II.6.19). The ring B is a principal ideal domain since it has only finitely many prime ideals ([30], III.2.12) and if $v \in B$ is such that $\sigma(v) = v$ for all $\sigma \in H$, then $v \in \mathbb{Z}_{(p)}$. It is easy to check that the p-part of the group $\Phi(M)$ is isomorphic to $\mathbb{Z}_{(p)}^n/M(\mathbb{Z}_{(p)}^n)$.

Assume that $K/\mathbb{Q}$ is Galois. There exist in B prime elements π_i, $i=1,\ldots,s$ (pairwise not associates), and a unit $\alpha\in B$, such that $p = \alpha(\pi_1\cdot\ldots\cdot\pi_s)^e$ with $e>0$ and $es \mid [K:\mathbb{Q}]$ ([30], III.8.1). The ideals (π_i) are the only maximal ideals of B.

Lemma 2.14. *Let λ denote an eigenvalue of an integer matrix M of rank n, or of rank $n-1$ with $r > 0$ as in 2.2. Assume $K/\mathbb{Q}$ Galois. Suppose that there exists a prime p dividing $L(\lambda)$ such that in B, $p = \alpha\pi_1 \cdot \ldots \cdot \pi_{[K:\mathbb{Q}]}$, with $\pi_1 \mid \lambda$, and $\pi_i \nmid \lambda$ for $i = 2, \ldots, [K:\mathbb{Q}]$ ((π_i), $i = 1, \ldots, [K:\mathbb{Q}]$, distinct prime ideals, and $\alpha \in B^*$). Let $w \in B^n$ be an eigenvector of M. Write the transpose of w as $(w_1, \ldots, w_n)$, and assume that the ideal in B generated by $w_1, \ldots, w_n$ is B. If M has rank $n-1$, assume in addition that $p \nmid r$. Then the class of $t(w)$ in $\mathbb{Z}^n_{(p)}/M(\mathbb{Z}^n_{(p)})$ has order $p^{\mathrm{ord}_p(L(\lambda))}$.*

Proof. We proceed as in 2.3 (1). Suppose that there exists a vector $S \in \mathbb{Z}^n_{(p)}$ and $c \in \mathbb{Z}_{(p)}$ dividing $L(\lambda)$ such that $MS = ct(w)$. Then $M((L(\lambda)/c)S - u(w)) = 0$, and we can find $d \in \mathbb{Z}_{(p)}$ such that $(L(\lambda)/c)S - u(w) = dR$. Since $\sigma(w)$ is an eigenvector for M, the dot product $u(w) \cdot R'$ is trivial. Taking the dot product of the latter equality with the vector R' shows that

$$(L(\lambda)/c)(S \cdot R) = dr.$$

It follows that $\frac{L(\lambda)}{c\gcd(L(\lambda)/c, r)}$ divides d.

Since $p \nmid r$, we find that $\mathrm{ord}_p(c) < \mathrm{ord}_p(L(\lambda))$ if and only if $p \mid \frac{L(\lambda)}{c\gcd(L(\lambda)/c, r)}$. Suppose that $\mathrm{ord}_p(c) < \mathrm{ord}_p(L(\lambda))$. Then p divides the coefficients of $u(w)$ since $u(w) = (L(\lambda)/c)S - dR$ has all its coefficients divisible by $\frac{L(\lambda)}{c\gcd(\lambda/c, r)}$. Thus π_1 must divide the coefficients of $u(w) := \sum_{\sigma \in H} \frac{L(\lambda)}{\sigma(\lambda)}\sigma(w)$.

Our additional hypothesis on λ (which implies that $L(\lambda) = N(\lambda)$) shows that if $\sigma \neq \mathrm{id}$, then $\pi_1 \mid \sigma(\frac{L(\lambda)}{\lambda})$, and $\pi_1 \nmid \frac{L(\lambda)}{\lambda}$. Hence, $\pi_1 \mid \frac{L(\lambda)}{\lambda} w_i$ for each $i = 1, \ldots, n$, implying that $\pi_1 \mid w_i$ for all $i = 1, \ldots, n$. This is a contradiction and, thus, $\mathrm{ord}_p(c) = \mathrm{ord}_p(N(\lambda))$, so that $t(w)$ has order $p^{\mathrm{ord}_p(N(\lambda))}$, as desired. □

Example 2.15 The eigenvalues of M are not, in general, related to $|\Phi(M)|$ when $r = 0$. Indeed, consider the matrix

$$M = \begin{pmatrix} 4 & 1 & 10 & 3 \\ 4 & 1 & 1 & 3 \\ 1 & 0 & 0 & 1 \\ 3 & 1 & 1 & 2 \end{pmatrix}.$$

The reader can verify that $\mathrm{char}_M(t) = t^2(t^2 - 7t - 13)$ and $\Phi(M) = \mathbb{Z}/9\mathbb{Z}$. The matrix has rank $n-1$, with $R = (1, -1, 0, -1)$ and $R' = (0, 1, -1, -1)$, so $r = 0$. The prime $p = 13$ satisfies the hypotheses of the lemma regarding its factorization in $\mathcal{O}_{\mathbb{Q}(\lambda)}$, but $\Phi(M)$ does not contain an element of order 13.

Example 2.16 Consider the graph G, without multiple edges, on $n = 26$ vertices, obtained as follows. Link a vertex v_1 to a vertex v_2 by three edges, and then divide each edges in 9. The resulting graph has 26 vertices. Add one more edge between v_1 and v_2 to get the graph G, with $\Phi(G) = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/108\mathbb{Z}$. The characteristic polynomial of G is

$$(t-3)^2(t^3 - 6t^2 + 9t - 3)^2(t^5 - 14t^4 + 69t^3 - 144t^2 + 117t - 24)\times$$
$$\times(t-1)^2(t^3 - 6t^2 + 9t - 1)^2(t^4 - 10t^3 + 33t^2 - 40t + 13)t.$$

The results of this section produce elements of order 3 in $\Phi(G)$: two 'independent' such elements from the factor $(t-3)^2$ (see 2.3), and one element each from the factors $(t^3 - 6t^2 + 9t - 3)$ and $(t^5 - 14t^4 + 69t^3 - 144t^2 + 117t - 24)$ (see 2.11). Each of these elements generates a subgroup of order 3. None of these subgroups is a direct factor of $\Phi(G)$. Note that $\Phi(G)$ has an element of order 27, so that the bound in 2.6 for the 3-part of the exponent of $\Phi(G)$ is achieved.

Let G^c denote the complement of G in K_{26}. The 5-part of the group $\Phi(G^c)$ is isomorphic to $\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. In particular, the group $\Phi(G^c)$ cannot be generated by 2 elements, even though the group $\Phi(G)$ can, and the multiplicities of the eigenvalues of G and G^c are the same (see 2.5). The characteristic polynomial of G^c is

$$(t^5 - 116t^4 + 5373t^3 - 124214t^2 + 1433185t - 6602130)(t-25)^2(t-23)^2\times$$

$$\times(t^3-72t^2+1725t-13753)^2(t^3-72t^2+1725t-13751)^2(t^4-94t^3+3309t^2-51700t+302497)t.$$

For the prime $p = 5$ (which is coprime to $n = 26$), the exponent of the 5-part of $\Phi(G^c)$ strictly divides the 5-part of the product of the distinct eigenvalues of G^c (the bound given in 2.6 for the exponent).

Example 2.17 We show in this example how to associate to each graph H on n vertices a graph G on $2n$ vertices whose group $\Phi(G)$ cannot be generated by fewer than $n-1$ elements.

Let H be a graph with adjacency matrix A and Laplacian eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n = 0$. Let d_i denote the degree of the i-th vertex. Consider the graph G with Laplacian matrix

$$\begin{pmatrix} 2D - A & -A \\ -A & 2D - A \end{pmatrix}.$$

The Laplacian eigenvalues of G are determined in [18] 3.6, and consists of $2\lambda_i$ and $2d_i$, for $i = 1, \ldots, n$. For instance, an eigenvector w for $2d_1$ is the transpose of $(1, 0, \ldots, 0, -1, 0, \ldots, 0)$, with -1 in the $(n+1)$-position. Since $w \cdot w = 2$, we can conclude from 2.3 (1) that the class of w in $\Phi(G)$ has order d_1 or $2d_1$.

We note that if H has a non-integer eigenvalue λ, then the eigenvalue 2λ of G has the property that $L(2\lambda) < N(2\lambda)$. Indeed, it is easy to check that for any algebraic integer λ of degree d and any integer $s > 0$, $N(s\lambda) = s^d N(\lambda)$, while $L(s\lambda) = sL(\lambda)$.

Straightforward row and column operations reduce the Laplacian of G to the matrix

$$N := \begin{pmatrix} 2D & 0 \\ -A & 2D - 2A \end{pmatrix}.$$

Let $\mathbb{Z}^{2n} \to \mathbb{Z}^n$ denote the projection onto the first n coordinates. This map induces a surjective group homomorphism $\mu : \mathbb{Z}^{2n}/\mathrm{Im}(N) \to \mathbb{Z}/2d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2d_n\mathbb{Z}$. Since $\Phi(G) \subseteq \mathbb{Z}^{2n}/\mathrm{Im}(N)$ we obtain a group homomorphism $\Phi(G) \to \mathbb{Z}/2d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2d_n\mathbb{Z}$. The image I of this latter homomorphism cannot be generated by fewer than $n-1$ elements. Indeed, the quotient of $\mathbb{Z}^{2n}/\mathrm{Im}(N)$ by $\Phi(G)$ is cyclic. Hence, the quotient of $\mathbb{Z}/2d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2d_n\mathbb{Z}$ by I is also cyclic. Therefore, the image cannot be generated by fewer than $n-1$ elements.

The fact that $\Phi(G)$ cannot be generated by fewer than $n-1$ elements (even when $\Phi(H)$ is cyclic) is not due, in general, to the presence of an integer eigenvalue of G with high multiplicity. For a general group $\Phi(G)$, the presence of a large number of integer eigenvalues with a common factor, or the presence of eigenvalues λ with $L(\lambda) < N(\lambda)$, could contribute distinct factors to the group $\Phi(G)$.

3. Strongly regular graphs

Connected graphs having only three distinct Laplacian eigenvalues are discussed in [16]. Such a graph is regular if and only if it is strongly regular ([16], 2.4). It is natural to wonder whether the Smith normal form of a graph with such restricted eigenvalues could be completely determined. It turns out that even though the eigenvalues are prescribed, the Smith normal form can vary. We develop in this section further relationships between

eigenvalues and Smith normal forms to be able to completely determine the Smith normal form of a conference graph on a squarefree number of vertices.

Let G be a (connected) strongly regular graph with parameters (n, k, a, c) (see, e.g., [21], chapter 10). Let k, θ, and τ, denote the distinct eigenvalues of the adjacency matrix A of G. The eigenvalues θ and τ are the roots of $x^2 - (a - c)x - (k - c)$. Since G is k-regular, the non-zero eigenvalues of the Laplacian matrix of G are $k-\theta$ and $k-\tau$. They are the roots of $x^2 - (a - c - 2k)x + nc$ (use (10.1) in [21]).

Lemma 3.1. *Assume that both θ and τ are integers, and that G has a connected complement. Then both integer Laplacian eigenvalues $k - \theta$ and $k - \tau$ are not coprime to n.*

Proof. Since G is connected, $c > 0$ and $a < k - 1$ ([21], 10.1.1). Moreover, since the complement of G, of type $(n, \bar{k}, \bar{a}, \bar{c})$, is connected, $k > c$; otherwise, $\bar{a} := (\bar{k}-1)+(c-k) \geq \bar{k} - 1$ contradicts the fact that the complement is connected.

Since $(k - \theta)(k - \tau) = nc$ and $c > 0$, at least one eigenvalue of the Laplacian is not coprime to n. If $\gcd(k - \theta, n) = 1$, then $k - \theta$ divides c. Let us show that $k - \theta$ cannot divide c. Suppose, *ab absurdo*, that there exists an integer e such that $e(k - \theta) = c$. We find that $\theta = k - c/e \geq k - c > 0$. As recalled above, $\theta\tau = c - k$. Solving for τ, we find that $\tau = -\frac{k-c}{k-c/e}$. Since τ is an integer, we obtain that $e = 1$ and $\tau = -1$. But then $\theta = k - c$ and $\theta + \tau = a - c = k - c - 1$ implies that $a = k - 1$, a contradiction. □

It may happen that $k - \theta$ and $k - \tau$ both divide n (in which case $c \mid n$ also). On the other hand, there are many parameters (n, k, a, c) where at least one of $k - \theta$ and $k - \tau$ is divisible by a prime p with $p \nmid n$. The symplectic graphs $\mathrm{Sp}(2r)$ ([21], 10.12.1) have this property for $p = 2$. These graphs have parameters $(2^{2r} - 1, 2^{2r-1}, 2^{2r-2}, 2^{2r-2})$, with eigenvalues $k - \theta = 2^{r-1}(2^r - 1)$ and $k - \tau = 2^{r-1}(2^r + 1)$.

Corollary 3.2. *Assume that G is a strongly regular graph with parameters (n, k, a, c). Then $\Phi(G)$ is killed by nc.*

When both (adjacency) eigenvalues θ and τ are integers, $\Phi(G)$ contains subgroups isomorphic to $(\mathbb{Z}/(k - \theta)\mathbb{Z})^{m(\theta)-1}$ and $(\mathbb{Z}/(k - \tau)\mathbb{Z})^{m(\tau)-1}$. If there exists a prime p with $p \mid (k - \theta)$ and $p \nmid n$, then $\Phi(G)$ contains a subgroup isomorphic to $(\mathbb{Z}/p^{\mathrm{ord}_p(k-\theta)}\mathbb{Z})^{m(\theta)}$.

Proof. Apply 2.3 and 2.6. □

A conference graph G is a strongly regular graph of the form (n, k, a, c) with $a = c - 1$, $k = 2c$, and[1] $n = 4c+1$; the multiplicities of $k-\theta$ and $k-\tau$ are equal to k. The Laplacian eigenvalues of G are $\lambda = (n + \sqrt{n})/2$ and $\bar{\lambda} = (n - \sqrt{n})/2$, with norm $(n^2 - n)/4 = nc$. Computations by Nathan Walters using Maple for Paley graphs on a prime number of vertices lead to the explicit formula of our next result.

Proposition 3.3. *Let G be a conference graph (n, k, a, c). The group $\Phi(G)$ contains a subgroup isomorphic to $(\mathbb{Z}/c\mathbb{Z})^{2c}$, and is killed by nc. When n is square free, then*

$$\Phi(G) = (\mathbb{Z}/c\mathbb{Z})^k \oplus (\mathbb{Z}/n\mathbb{Z})^{k-1}.$$

We postpone the proof of 3.3 to 3.8, after we have proved the more general result 3.7.

[1]It is known that n is the sum of two squares or, equivalently, that any prime factor p of n congruent to 3 modulo 4 appears with an even power in the factorization of n. This implies for instance that $c \not\equiv 5$ or 8 (mod 9), since for such a c, $4c + 1$ is exactly divisible by 3.

Remark 3.4 Computations were done by Grant Fiddyment in the case of the 15 strongly regular graphs with parameters $(25, 12, 5, 6)$ (see [37] for the list of graphs); in this case, $nc = 150$, $\frac{n-1}{4} = 6$, and the eigenvalues are integral: 15 and 10. As predicted by 2.3, $\Phi(G)$ contains subgroups isomorphic to $(\mathbb{Z}/10\mathbb{Z})^{11}$, $(\mathbb{Z}/15\mathbb{Z})^{11}$, and $(\mathbb{Z}/6\mathbb{Z})^{12}$. The prime-to-5 part of all groups is $(\mathbb{Z}/6\mathbb{Z})^{12}$. There are ten such graphs where the 5-part of the group is

$$(\mathbb{Z}/25\mathbb{Z})^{10} \oplus (\mathbb{Z}/5\mathbb{Z})^2,$$

four such graphs where the 5-part of the group is

$$(\mathbb{Z}/25\mathbb{Z})^{9} \oplus (\mathbb{Z}/5\mathbb{Z})^4,$$

and one graph where the 5-part of the group is

$$(\mathbb{Z}/25\mathbb{Z})^{7} \oplus (\mathbb{Z}/5\mathbb{Z})^8.$$

Note that this example shows that the eigenvalues of a matrix M of rank $n-1$ do not determine the structure of the group $\Phi(M)$. Moreover, the theoretical results of the previous section only establish the existence of elements of order 5 in $\Phi(G)$, in the form of two subgroups isomorphic to $(\mathbb{Z}/5\mathbb{Z})^{11}$, and this example indicates that elements of order 5^2 are plentiful. Brandon Samples determined that the last group in the above list is the group of the Paley graph on $\mathbb{F}_{5^2}$.

3.5 Let M be any $(n \times n)$-integer matrix of rank $n-1$. Let $\mathrm{char}_M(x)$ denote the characteristic polynomial of M. Let $f(x) = x^d + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ denote a factor of $\mathrm{char}_M(x)/x$. Write $f(x) = xg(x) + a_0$. Consider the following exact sequence:

$$0 \longrightarrow \mathrm{Im}(M)/\mathrm{Im}(Mg(M)) \longrightarrow \mathbb{Z}^n/\mathrm{Im}(Mg(M)) \longrightarrow \mathbb{Z}^n/\mathrm{Im}(M) \longrightarrow 0.$$

The eigenvalues of $Mg(M)$ are $\{\lambda g(\lambda), \mathrm{char}_M(\lambda) = 0\}$. (It may happen in particular that $Mg(M)$ has rank smaller than $n-1$.) If N is any $(n \times n)$-integer matrix, let us denote by $\Phi(N)$ the torsion subgroup of $\mathbb{Z}^n/\mathrm{Im}(N)$. Taking the torsion subgroups in the above exact sequence results in the exact sequence of finite abelian groups:

$$0 \longrightarrow (\mathrm{Im}(M)/\mathrm{Im}(Mg(M)))_{\mathrm{tors}} \longrightarrow \Phi(Mg(M)) \longrightarrow \Phi(M).$$

Suppose that $f(\lambda) = 0$, and that w is an eigenvector of M for λ. Then w is an eigenvector of $Mg(M)$ for $-a_0$. Indeed, if $Mw = \lambda w$, then $Mg(M)w = -a_0 w$, since $f(M)w = f(\lambda)w = 0$. Since a_0 is an integer and $Mg(M)$ is an integer matrix, we find that there exists an eigenvector $v \in \mathbb{Z}^n$ of $Mg(M)$ for a_0, and that the class of v in $\mathbb{Z}^n/\mathrm{Im}(Mg(M))$ is in fact in $\Phi(Mg(M))$, (of order dividing a_0, since $Mg(M)v = -a_0 v$). The image in $\Phi(M)$ of the class of v in $\Phi(M(gM))$ is thus an interesting element of $\Phi(M)$ 'related to the eigenvectors' of λ.

Consider the natural map $\mathbb{Z}^n/\mathrm{Im}(Mg(M)) \longrightarrow \mathbb{Z}^n/\mathrm{Im}(M) \times \mathbb{Z}^n/\mathrm{Im}(g(M))$, and denote by

$$q : \Phi(Mg(M)) \longrightarrow \Phi(M) \times \Phi(g(M))$$

the map it induces on the torsion subgroups. As we shall see below, the map q is not always an isomorphism, but it does provide useful information on $\Phi(M)$ in some cases.

Consider the following special case. Let M be any $(n \times n)$-integer matrix of rank $n-1$ with $r > 0$. Assume that $\mathrm{char}_M(x) = xf(x)^\mu$. Then the group $\Phi(M)$ has order $|a_0|^\mu/r$, and $r \mid a_0$ (2.1). The matrix $Mg(M)$ has rank $n-1$, with characteristic polynomial $x(x+a_0)^{d\mu}$. If $MR = 0$ and ${}^tR'M = 0$, then $Mg(M)R = 0$ and ${}^tR'Mg(M) = 0$. We can apply 2.1 again to find that the group $\Phi(Mg(M))$ has order $|a_0|^{d\mu}/r$.

Let $\lambda_1, \ldots, \lambda_d$, denote the non-zero roots of $f(x)$. When $a_1 \neq 0$, the matrix $g(M)$ is invertible, and

$$|\det(g(M))| = |g(0)\prod_{i=1}^{d} g(\lambda_i)^{\mu}| = |a_1 \prod_{i=1}^{d}(-a_0/\lambda_i)^{\mu}| = |a_1 a_0^{d\mu-\mu}|.$$

As we see in this example when $a_1 \neq 0$, the map q is not an isomorphism, since the integers $|\Phi(Mg(M))|$ and $|\Phi(M)||\Phi(g(M))|$ differ by a factor $|a_1|$.

When M is the Laplacian of a graph, the non-zero eigenvalues are all positive. Thus the coefficient a_1 of any factor $f(x)$ of $\mathrm{char}_M(x)/x$ is non-zero.

Proposition 3.6. *Keep the notation of 3.5, and assume $a_1 \neq 0$. The kernel of the map $\mathbb{Z}^n/\mathrm{Im}(Mg(M)) \longrightarrow \mathbb{Z}^n/\mathrm{Im}(M) \times \mathbb{Z}^n/\mathrm{Im}(g(M))$ is killed by a_1, and the natural map*

$$q : \Phi(Mg(M)) \longrightarrow \Phi(M) \times \Phi(g(M))$$

induces an isomorphism on the prime-to-a_1 part of these groups.

Proof. Write $g(x) = xh(x) + a_1$. Suppose that $u \in \mathbb{Z}^n$ is such that there exists v and w in $\mathbb{Z}^n$ with $Mv = u$ and $g(M)w = u$. Then $Mv = (Mh(M) + a_1)w$, from which we get $a_1 w = M(v - h(M)w)$. Thus, $a_1 u = a_1 g(M)w = g(M)M(v - h(M)w)$. It follows that the class of $a_1 u$ is trivial in $\mathbb{Z}^n/\mathrm{Im}(Mg(M))$. In particular, the class of u is in $\Phi(Mg(M))$.

Let $v \in \mathbb{Z}^n$ represent an element of $\Phi(M)$ of order s, and let $w \in \mathbb{Z}^n$ represent an element of $\Phi(g(M))$ of order t. Consider the element $u := g(M)v - Mh(M)w$. Clearly, $u \equiv a_1 v \pmod{\mathrm{Im}(M)}$, and $u \equiv a_1 w \pmod{\mathrm{Im}(g(M))}$. We claim that u represents an element of $\Phi(Mg(M))$. Indeed, the class of stu is in the kernel of the map $\mathbb{Z}^n/\mathrm{Im}(Mg(M)) \to \mathbb{Z}^n/\mathrm{Im}(M) \times \mathbb{Z}^n/\mathrm{Im}(g(M))$ by our choice of v and w, and we showed above that this kernel is killed by a_1. It follows that u has finite order in $\mathbb{Z}^n/\mathrm{Im}(Mg(M))$, as desired.

Restrict now the map q to the prime-to-a_1 part of $\Phi(Mg(M))$. It is clearly injective since the order of an element in the kernel divides a_1. Given any element $(\bar{v}', \bar{w}')$ in $\Phi(M) \times \Phi(g(M))$ of order prime to a_1, there exists $(\bar{v}, \bar{w})$ in $\Phi(M) \times \Phi(g(M))$ such that $a_1(\bar{v}, \bar{w}) = (\bar{v}', \bar{w}')$. The above discussion shows that we can find $u \in \mathbb{Z}^n$ whose class modulo $\mathrm{Im}(Mg(M))$ is in $\Phi(Mg(M))$ and such that $q(u) = (a_1\bar{v}, a_1\bar{w}) = (\bar{v}', \bar{w}')$. Thus, the map q is surjective when restricted to the prime-to-a_1-parts. □

Corollary 3.7. *Let M be a symmetric $(n \times n)$- integer matrix of rank $n-1$ with $r > 0$. Assume that $\mathrm{char}_M(x) = xf(x)^{\mu}$ and $a_1 \neq 0$.*

(a) *The group $\Phi(Mg(M))$ is isomorphic to $(\mathbb{Z}/a_0\mathbb{Z})^{\mu d-1} \times \mathbb{Z}/\frac{a_0}{r}\mathbb{Z}$.*
(b) *Let b and c denote, respectively, the largest divisor of r, and the largest divisor of a_0/r, coprime to a_1. Then $\Phi(M)$ contains a subgroup isomorphic to $(\mathbb{Z}/bc\mathbb{Z})^{\mu-1} \times \mathbb{Z}/c\mathbb{Z}$.*

Proof. (a) Let $\Phi := \Phi(Mg(M))$. We already discussed above that $r \mid a_0$ and $|\Phi| = |a_0|^{d\mu}/r$. Proposition 2.3 (2) shows that Φ contains a subgroup H isomorphic to $(\mathbb{Z}/a_0\mathbb{Z})^{d\mu-1}$. Proposition 2.6 shows that Φ is killed by $|a_0|$. Consider the quotient Φ/H. It has order $|a_0|/r$. To prove (a), it remains to show that there exists an element in Φ of order $|a_0|/r$ whose image in Φ/H generates Φ/H. To prove this fact, pick any $\varphi \in \Phi$ whose image in Φ/H generates Φ/H. Then $\frac{|a_0|}{r}\varphi \in H$, and since $|a_0|$ kills Φ, the order of $\frac{|a_0|}{r}\varphi$ divides r. Since H is isomorphic to $(\mathbb{Z}/a_0\mathbb{Z})^{d\mu-1}$, we find that any element of order dividing r can be divided by $\frac{|a_0|}{r}$ in H, that is, there exists $\epsilon \in H$ such that $\frac{|a_0|}{r}\epsilon = \frac{|a_0|}{r}\varphi$. It follows that the element $\varphi - \epsilon$ has order exactly $\frac{|a_0|}{r}$ in Φ, and its image in Φ/H generates Φ/H, as desired.

(b) The prime-to-a_1 part Φ' of the group $\Phi(Mg(M))$ is isomorphic to $(\mathbb{Z}/bc\mathbb{Z})^{\mu d-1} \times \mathbb{Z}/c\mathbb{Z}$. Proposition 3.6 shows that the prime-to-a_1 part $\Phi(M)'$ of $\Phi(M)$ is a direct summand of Φ' of order c^μ. Hence, $\Phi(M)'$ can only be isomorphic to a group of the form $(\mathbb{Z}/bc\mathbb{Z})^\alpha$, or $(\mathbb{Z}/bc\mathbb{Z})^\beta \times \mathbb{Z}/c\mathbb{Z}$ for some integers α and β. Since $|\Phi(M)| = |a_0|^\mu/r$, we find that $\Phi(M)'$ is isomorphic to $(\mathbb{Z}/bc\mathbb{Z})^{\mu-1} \times \mathbb{Z}/c\mathbb{Z}$. □

3.8 *Proof of 3.3.* The characteristic polynomial of G is $x(x^2 - nx + nc)^{2c}$. When n is a perfect square, we can apply 2.3 to all primes dividing $(\sqrt{n}-1)/2$ and $(\sqrt{n}+1)/2$. Since $(\sqrt{n}-1)/2$ and $(\sqrt{n}+1)/2$ are coprime and $c = (n-1)/4$, we find that $\Phi(G)$ contains a subgroup isomorphic to $(\mathbb{Z}/c\mathbb{Z})^{2c}$. When n is not a perfect square, this statement follows directly from 3.7. When n is square free, the fact that nc kills $\Phi(G)$ with $|\Phi(G)| = (nc)^{2c}/n$ forces $\Phi(G)$ to contain a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2c-1}$. □

4. How often is $\Phi(G)$ cyclic?

Let G be a connected graph with n vertices $v_1, \ldots, v_n$, m edges (adjacent vertices may be linked by more than one edge), and Laplacian M. Should one expect that $\Phi(G)$ is 'often' cyclic for a randomly chosen graph? More generally, it would be of interest to know for a given r the probability that $\Delta_r(M) = 1$. (Recall that $\Delta_r(M)$ denote the greatest common multiple of the determinants of all $(r \times r)$-minors of M, and that $\Phi(G)$ is cyclic if and only if $\Delta_{n-2}(M) = 1$.) We formulate in this section three precise probabilities of interest concerning the behaviour of the structure of $\Phi(G)$ in the set of all isomorphism classes of graphs, in 4.1, 4.4, and 4.9.

4.1 For each integer n, let $\mathcal{G}_n^v$ be the set of all isomorphism classes of finite connected graphs G having n vertices and no multiple edges, and having vertex connectivity at least 2 (for any vertex v of G, the topological space $G \setminus \{v\}$ is connected). Then $\mathcal{G}_n^v$ is a finite set. Let $\mathcal{C}_n^v$ denote the subset of $\mathcal{G}_n^v$ consisting of all the graphs G whose group $\Phi(G)$ is cyclic. Consider

$$\rho_v(n) := \frac{|\mathcal{C}_n^v|}{|\mathcal{G}_n^v|}. \tag{2}$$

Since the cycle C_n on n vertices has $\Phi(C_n)$ cyclic of order n, we find that $\rho_v(n) > 0$. It would be of interest to know whether the limits $\lim_{n\to\infty} \rho_v(n)$ and $\lim_{n\to\infty} \frac{\sum_{i=1}^n |\mathcal{C}_i^v|}{\sum_{i=1}^n |\mathcal{G}_i^v|}$ exist.

Had we not asked for $\mathcal{G}_n^v$ to contain only graphs having vertex connectivity at least 2, it would be obvious that $|\mathcal{C}_n^v| < |\mathcal{C}_{n+1}^v|$, so that $\lim_{n\to\infty} |\mathcal{C}_n^v| = \infty$. Indeed, any graph G on n vertices and cyclic group $\Phi(G)$ produces many graphs G' on $n+1$ vertices with cyclic group $\Phi(G')$: simply attach to any vertex of G a new vertex of degree 1. With our more restrictive definition:

Proposition 4.2. *With the above notation,* $\lim_{n\to\infty} |\mathcal{C}_n^v| = \infty$, *and* $\lim_{n\to\infty} |\mathcal{G}_n^v \setminus \mathcal{C}_n^v| = \infty$.

Proof. Consider a cycle G on N vertices, and choose two adjacent vertices v and v'. Pick a new vertex w and link it to both v and v' to obtain a graph G' on $N+1$ vertices, without multiple edges, and with vertex connectivity at least 2. This is an example of a graph obtained from G by adding a chain, as in 6.6. Since $\Phi(G)$ is cyclic, so is $\Phi(G')$. The maximum degree of a vertex of G' is 3. We can continue the process of adding chains (as in 6.5) ℓ times. We can construct in this way at least $\ell - 1$ non-isomorphic graphs on $N+\ell$ vertices, each with cyclic group Φ: indeed, for $M \in [4, \ell+2]$, we can construct a graph with maximum degree M. These $\ell - 1$ graphs are obviously pairwise not isomorphic, and $\lim_{n\to\infty} |\mathcal{C}_n^v| = \infty$.

For each integer $n > 10$, there exist about $3n/10$ ways to write $n = x + y$ with $y > x > n/5$ and $n/2 < y < n/2 + 3n/10$. For each such pair (x, y), there exists at least one connected graph G with x vertices and y edges, with vertex connectivity at least 2, and with $\beta(G) = y - x + 1 > 1$ (start for example with a cycle on x vertices, and keep adding edges to it). Now divide each edge of G in two (i.e., add one vertex on each edge of G). The resulting graph G' has $n = x + y$ vertices, and $2y$ edges, and is without multiple edges. Since $\beta(G) > 1$, the group $\Phi(G')$ is not cyclic ([28], 5.1). Since G' has $x + y$ vertices, we have constructed in this way about $3n/10$ non-isomorphic graphs on n vertices whose associated groups are not cyclic. □

Another way of producing many graphs of a given size with non-cyclic groups Φ is given in 2.17. A criterion for a graph to have $\Phi(G)$ contain $(\mathbb{Z}/r\mathbb{Z})^{\beta(G)}$ is given in [12], 7.5.1.

4.3 The following numerical data for some variant of $\rho_v(n)$ was obtained by sophomore Grant Fiddyment using the tables of non-isomorphic graphs downloaded from Brendan McKay's web page [31]. The table below pertains only to connected graphs on n vertices contained in the complete graph K_n and *without* a vertex of degree 1.

The second line of the table exhibits the proportion of such graphs whose complexity $|\Phi(G)|$ is squarefree (in which case $\Phi(G)$ is automatically cyclic). The third line exhibits the proportion of such graphs whose group $\Phi(G)$ is cyclic. The fourth line of the table exhibits the proportion of graphs whose group $\Phi(G)$ is cyclic among all graphs (on n vertices *without* a vertex of degree 1) whose complexity $|\Phi(G)|$ is not squarefree.

n	5	6	7	8	9	10
% squarefree	27.27	29.51	28.60	32.68	37.74	41.49
% cyclic	45.45	52.46	56.80	62.68	68.02	72.41
% cyclic, not squarefree	25	32.56	39.50	44.57	48.64	52.84

This data suggests that, even among the graphs having complexity that is not squarefree, one could expect to find a substantial proportion of graphs that are cyclic.

4.4 Consider, for each integer κ, the set $\mathcal{G}_\kappa$ of all isomorphism classes of finite connected graphs G having $\kappa(G) = \kappa$, and having vertex connectivity at least 2. Then $\mathcal{G}_\kappa$ is a finite set (use 4.5). Let $\mathcal{C}_\kappa$ denote the subset of $\mathcal{G}_\kappa$ consisting of all the graphs G whose group $\Phi(G)$ is cyclic. Consider

$$\rho(\kappa) := \frac{|\mathcal{C}_\kappa|}{|\mathcal{G}_\kappa|}. \tag{3}$$

Since the cycle C_κ on κ vertices has $\Phi(C_\kappa)$ cyclic of order κ, we find that $\rho(\kappa) > 0$. It is clear that if κ is a squarefree integer, then $\rho(\kappa) = 1$. Is there a universal constant $c > 0$ such that $\rho(\kappa) > c$ for all κ? It would also be of interest to know whether the following limit exists: $\lim_{\kappa\to\infty} \frac{\sum_{i=1}^{\kappa} |\mathcal{C}_i|}{\sum_{i=1}^{\kappa} |\mathcal{G}_i|}$.

Proposition 4.5. *Let G be a connected graph with vertex connectivity at least 2. Then $\kappa(G) \geq m$.*

Proof. When G has two vertices and m edges, $\kappa(G) = m$. When G has three vertices u, v, and w, with $\{uv\} = a$, $\{vw\} = b$, and $\{wu\} = c$, the vertex connectivity is at least 2 if $abc \neq 0$. In this case, $\kappa(G) = ab + bc + ac \geq a + b + c$. When G has $n > 3$ vertices and has vertex connectivity at least 2, consider the graph G_1 obtained from G by removing all c edges between a given pair of vertices $\{v, v'\}$ of G. Then $\kappa(G_1) \geq 1$ since G_1 is connected

by hypothesis. The graph G_2 obtained from G_1 by identifying v and v' has $n-1$ vertices, and our proof will proceed by induction once we have proved the following claim.

It is always possible to find a pair of vertices $\{v, v'\}$ of G such that the vertex connectivity of G_2 is at least 2. Indeed, the vertex connectivity of G_2 is always greater than or equal to the vertex connectivity of G minus 1. Thus, to prove our claim, it suffices to show it for graphs G of vertex connectivity 2. Assume that a pair $\{v, v'\}$ of adjacent vertices is such that the associated graph G_2 has vertex connectivity 1. Then $V(G)\backslash\{v, v'\} = A_1 \sqcup \cdots \sqcup A_r$ for some $r > 1$, with $A_1, \ldots, A_r$ nonempty pairwise disjoint sets of vertices of G producing pairwise disjoint connected subgraphs $H_1, \ldots, H_r$ of G such that the complement in G of $\cup_{i=1}^r H_i$ is the set of edges of G having an end point in $\{v, v'\}$ union the set $\{v, v'\}$. Since G is connected, we may assume that v is connected in G to a vertex $a \in A_1$. Then v' must be connected in G to a vertex $b \in A_i$ for some $i > 1$, otherwise G has vertex connectivity 1 since $G\backslash\{v\}$ would be disconnected. Consider now all (the finitely many) possible quadruples $(v, v', A_1 \ni v, A_i \ni v')$ constructed as above, and pick one where $\max(|A_1|, |A_i|)$ is maximal among all such quadruples $(v, v', A_1 \ni v, A_i \ni v')$. Without loss of generality, we may assume that $\max(|A_1|, |A_i|) = |A_i|$. Consider now the pair $\{v, a\}$. The vertices of A_i are still connected in $G \setminus \{v, a\}$, and also connected to v'. Thus, by maximality of $|A_i|$, we find that $V(G) \setminus \{v, a\}$ cannot be the disjoint union of nonempty subsets $A'_1, \ldots, A'_{r'}$ producing disjoint connected subgraphs of G. Hence, the vertex connectivity of the graph G_2, obtained by removing the edges between v and a and identifying the vertices v and a, is 2.

We proceed now by induction on the number $n > 3$ of vertices of G. Our claim above implies the existence of a pair of vertices (linked by $c > 0$ edges) such that the induction hypothesis can be applied to the associated graph G_2, so that $\kappa(G_2) \geq m - c$. We find then that $\kappa(G) = \kappa(G_1) + c\kappa(G_2) \geq 1 + c(m - c) \geq m$, since $m \geq c + 1$. □

□

Example 4.6 For each integer of the form $4(n-1)$, there exists several graphs G on $n > 2$ vertices with $\Phi(G)$ cyclic of order $4(n-1)$. Indeed, any graph G obtained from a cycle on n vertices by 'doubling' two existing edges is such a graph. To see this, first note that all such graphs G have the same dual G^*, with four vertices u, v, w, x, such that u is linked to v and x; and w is linked to v and x, and v linked to x by $n-2$ edges. The group $\Phi(G^*)$ is easily computed to be cyclic of order $4n-4$.

Note that as $n \to \infty$, the number of non-isomorphic graphs G constructed above with $\Phi(G)$ cyclic of order $4(n-1)$ tends to infinity. This statement is generalized in 4.8.

When $n = 3$, we obtain a graph with complexity 8. This graph, along with the cycle on 8 vertices and their duals, are the only graphs in $\mathcal{G}_8$, and we have $\mathcal{G}_8 = \mathcal{C}_8$.

Example 4.7 Consider the graph $G = G(x, y, z)$ having adjacency matrix

$$\begin{pmatrix} 0 & x & y \\ x & 0 & z \\ y & z & 0 \end{pmatrix}.$$

It is not difficult to check that $\kappa(G) = xy + yz + zx$, and that $\Phi(G)$ is cyclic if and only if $\gcd(x, y, z) = 1$. If $\gcd(x, y, z) \neq 1$, then $\Phi(G)$ is the product of two cyclic groups, of order $\gcd(x, y, z)$ and $(xy + yz + zx)/\gcd(x, y, z)$, respectively.

Taking $x = 1$ and $y = 1$, we find that $xy + yz + zx = 1 + 2z$ represents all odd positive integers greater than 1. Thus, the duals $G(1, 1, z)^*$ are graphs on $z + 1$ vertices with $\Phi(G(1, 1, z)^*)$ cyclic of order $2z + 1$. When $1 \leq x < y, z$, the duals $G(x, y, z)^*$ are without multiple edges, and are studied in [9], 9.6/10, or [29], 2.5.

It turns out that the quadratic form $xy + yz + zx$ represents all positive integers except $1, 2, 4, 6, 10, 18, 22, 30, 42, 58, 70, 78, 102, 130, 190, 210, 330, 462$, and possibly one additional integer (the latter possibility being ruled out when assuming the Generalized Riemann Hypothesis) [8]. In fact, much more is known about the quadratic form $xy+yz+zx$, allowing us to deduce the following proposition.

Proposition 4.8. *Let $\mathcal{C}_\kappa$ be as in 4.4. Then $\lim_{\kappa\to\infty} |\mathcal{C}_\kappa| = \infty$.*

Proof. Let $T(n)$ denote the set of integer solutions (x, y, z) of the equation $xy+yz+zx = n$ with $0 < x < y < z$ and $\gcd(x, y, z) = 1$. Let $h(d)$ denote the number of equivalence classes of primitive binary quadratic forms $ax^2 + by^2 + cz^2$ with $a > 0$ and $b^2 - 4ac = -d$. Let $w(n)$ denote the number of different prime factors in the factorization of n. Yuan [39] (as reported in Math Reviews MR1778804) showed that

$$2|T(n)| = h(-4n) - 2^{w(n)}$$

if n is odd or $8 \mid n$, and $2|T(n)| = h(-4n)-2^{w(n)-1}$ if n is even and $8 \nmid n$. (See also [8], proof of 3.1, when n is squarefree and even.) Chowla [13] proved that $\lim_{d\to\infty} h(d)2^{-w(d)} = \infty$. It follows from these results that $\lim_{n\to\infty} |T(n)| = \infty$. The proposition follows by applying the above statement to the graphs $G(x, y, z)$ introduced in 4.7. When $(x, y, z) \in T(n)$, such a graph has a cyclic group of order n. It is clear that two graphs $G(x, y, z)$ and $G(x', y', z')$ with (x, y, z) and (x', y', z') in $T(n)$ are not isomorphic if $(x, y, z) \neq (x', y', z')$ (since $(x, y, z) \in T(n)$ has $0 < x < y < z$ by hypothesis). □

4.9 A different statistics on the Smith normal form of Laplacians of graphs, of interest to algebraic geometers, is the following. Fix an integer β, and consider the set of all isomorphism classes of connected graphs G such that $\beta(G) = \beta$. What is the proportion of graphs in this set with $\Phi(G)$ cyclic? (See [11] for a relevant result.) To formulate a precise question, consider the set $\mathcal{B}_n$ of all isomorphism classes of connected graphs G on n vertices such that $\beta(G) = \beta$ (we could also further restrict $\mathcal{B}_n$ to consist only of the graphs without vertices of degree 1). Let $\mathcal{B}'_n$ denote the subset of $\mathcal{B}_n$ consisting of the graphs G with $\Phi(G)$ cyclic. Consider

$$\lim_{n\to\infty} \frac{\sum_{i=1}^n |\mathcal{B}'_i|}{\sum_{i=1}^n |\mathcal{B}_i|}.$$

To give an example where a related limit can be computed, consider the family of dual graphs $G^*(x, y, z)$, $0 < x \leq y \leq z$, with $G(x, y, z)$ introduced in 4.7. Each graph $G^*(x, y, z)$ has $\beta(G^*(x, y, z)) = 2$. When $x > 1$ or $y > x = 1$, the graph is without multiple edges and has vertex connectivity 2. Any graph G with $\beta(G) = 2$ and vertex connectivity 2 belongs to this family. We owe the proof of the next proposition to Andrew Granville.

Proposition 4.10. *Consider the set $D(n)$ of graphs $G^*(x, y, z)$, $0 < x \leq y \leq z$, with $x + y + z = n$. Let $C(n)$ denote the subset of $D(n)$ consisting of the graphs $G^*(x, y, z)$ with $\Phi(G^*(x, y, z))$ cyclic. Then*

$$\lim_{n\to\infty} \frac{\sum_{i=3}^n |C(i)|}{\sum_{i=3}^n |D(i)|} = \frac{1}{\zeta(3)} = 0.8319....$$

Proof. Recall that $\Phi(G^*(x, y, z))$ is cyclic if and only if $\gcd(x, y, z) = 1$. Abusing notation, we let

$$D(n) := \{(x, y, z) \in \mathbb{N}^3, 0 < x \leq y \leq z, x + y + z = n\},$$

and $C(n) = \{(x,y,z) \in D(n), \gcd(x,y,z) = 1\}$. For each $x \leq n/3$, we have $n - x = y + z \geq 2y$. We find that

$$|D(n)| = \sum_{i=1}^{\lfloor n/3 \rfloor} \lfloor (n-i)/2 \rfloor - (i-1) = n^2/12 + O(n).$$

Therefore,

$$\sum_{i=3}^{n} |D(i)| = n^3/36 + O(n^2).$$

If $(x,y,z) \in D(n)$ with $g := \gcd(x,y,z)$, then $(x/g, y/g, z/g) \in C(n/g)$, so that

$$|D(n)| = \sum_{g|n} |C(n/g)|.$$

By Möbius inversion, $|C(n)| = \sum_{d|n} \mu(d)|D(n/d)|$. Therefore

$$\begin{array}{rcl} \sum_{i=3}^{n} |C(i)| & = & \sum_{i=3}^{n} \sum_{d|i} \mu(d)[(i^2/12d^2) + O(i/d)] \\ & = & \frac{1}{12} \sum_{d \leq n} \mu(d) \sum_{3 \leq i \leq n, d|i} (i^2/d^2) + O(n^2) \\ & = & \frac{1}{12} \sum_{d \leq n} \mu(d) \sum_{m \leq n/d} m^2 + O(n^2) (\text{ writing } i = dm) \\ & = & \frac{1}{12} \sum_{d \leq n} \mu(d)((n/d)^3/3 + O((n/d)^2)) + O(n^2) \\ & = & \frac{n^3}{36} \sum_{d \leq n} \mu(d) \frac{1}{d^3} + O(n^2) \\ & = & \frac{n^3}{36}(1/\zeta(3)) + O(n^2), \end{array}$$

where we recall the identity $1/\zeta(s) = \sum_{d=1}^{\infty} \mu(d)/d^s$. Therefore,

$$(\sum_{i=3}^{n} |C(i)|)/(\sum_{i=3}^{n} |D(i)|) = 1/\zeta(3) + O(1/n).$$

Thus, the limit as $n \to \infty$ is $1/\zeta(3)$. □

5. Removing disjoint paths from a complete graph

We study in this section a family of subgraphs $G(n,a,b)$ of the complete graph K_n and completely determine the structure of the groups $\Phi(G(n,a,b))$. We also obtain information on the proportion of graphs $G(n,a,b)$ whose group $\Phi(G(n,a,b))$ is cyclic.

5.1 It is proved in [27], 5.3, that if G' is obtained from G by removing all edges of G between a given pair of vertices, then the minimal number of generators of $\Phi(G)$ and $\Phi(G')$ can differ by at most 1.

The complete graph K_n on n vertices has $\Phi(K_n) = (\mathbb{Z}/n\mathbb{Z})^{n-2}$. Starting with K_n and removing s edges $\{e_1, \ldots, e_s\}$ to obtain a graph G, we find that the group $\Phi(G)$ can be cyclic only when $s \geq n-3$. Moreover, if $s = n-3$ and $\Phi(G)$ is cyclic, then any graph obtained from K_n by removing $r < s$ edges in $\{e_1, \ldots, e_s\}$ has a group Φ minimally generated by $n-2-r$ elements and is thus not cyclic. This is the case for the class of graphs studied in this section.

Let a, b, and n be positive integers such that $a + b = n - 1$. Let $G(n,a,b)$ denote the graph obtained by removing from K_n the $n-3$ edges of two vertex-disjoint paths on a and b vertices, respectively. The complexity of such graph is well-known, and can be computed using a formula of Temperley ([5], 6.4). To be able to specify the structure of the group $\Phi(G(a,b,n))$, we introduce the following notation.

Let $k > 2$ be any positive integer and consider the $(k \times k)$-tridiagonal matrix

$$D_k := \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & & \vdots \\ 0 & 1 & \ddots & \ddots & 0 \\ \vdots & & \ddots & 0 & 1 \\ 0 & \dots & 0 & 1 & 1 \end{pmatrix}.$$

When $k = 2$ we set $D_k = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Write $\xi_m := \cos(2\pi/m) + i\sin(2\pi/m)$. The characteristic polynomial $\mathrm{char}(D_k)(x) := \det(x\mathrm{I}_k - D_k)$ of D_k can be computed explicitly as follows.

Proposition 5.2. *If $k \geq 2$, then $\mathrm{char}(D_k)(x) = \prod_{s=0}^{k-1}(x - (\xi_{2k}^s + \xi_{2k}^{-s}))$.*

Proof. We exhibit below the k distinct eigenvectors of D_k and their corresponding eigenvalue. First, $(1, \dots, 1)$ has eigenvalue 2. Then, for $s = 1, \dots, k-1$,

$$E_s := (1, \xi_{2k}^s, (\xi_{2k}^s)^2, \dots, (\xi_{2k}^s)^{k-1}) + ((\xi_{2k}^s)^{2k-1}, \dots, (\xi_{2k}^s)^{k+1}, (\xi_{2k}^s)^k)$$

has eigenvalue $\lambda_s = \xi_{2k}^s + \xi_{2k}^{-s}$. These statements can be checked directly. Note that the matrix D_k is, up to four coefficients, the adjacency matrix of a cycle on k vertices. The eigenvectors of this latter matrix are known (see [5], 3.5), and almost all eigenvalues have two linearly independent eigenvectors. Adding the two eigenvectors for the same eigenvalue gives an eigenvector for D_k for that eigenvalue. Then the matrix D_{2k} is, up to four coefficients, the direct sum of two matrices D_k. It turns out that the vectors E_s are obtained by truncating in half $k-1$ eigenvectors of D_{2k} constructed above. □

Remark 5.3 Much can be said a priori on the eigenvalues of D_k. The Perron-Frobenuis theorem shows that the absolute value of an eigenvalue λ of a non-negative matrix is bounded by the maximum of its row-sums. Thus, the eigenvalues of D_k are in $[-2, 2]$. Kronecker [25] showed that if a monic polynomial of degree k in $\mathbb{Z}[n]$ has $\lambda_1, \dots, \lambda_k$ real roots and all the roots are in $[-2, 2]$, then $\lambda_i = 2\cos(a_i\pi/b_i)$ for some integers a_i, b_i.

Since $\mathrm{char}(D_k)(x)$ is divisible by $(x-2)$, we let $h_k(x) := \mathrm{char}(D_k)(x)/(x-2)$.

Proposition 5.4. *Let $a, b \geq 2$ be such that $a + b = n - 1$. Then*

$$\Phi(G(n, a, b)) = \mathbb{Z}/\gamma\mathbb{Z} \times \mathbb{Z}/\delta\mathbb{Z},$$

with $\gamma \mid \delta$ and $\gamma\delta = n|h_a(2-n)h_b(2-n)|$. Moreover, γ divides $\gcd(|h_a(2-n)|, |h_b(2-n)|)$. When $\gcd(a, b) = 1$, $\Phi(G(n, a, b))$ is cyclic.

Proof. To show that the group $\Phi(G)$ is cyclic, it suffices to prove that $\Delta_{n-2} = 1$. In fact, it suffices to exhibit t $(n \times n)$-matrices N_i row and column equivalent to M, and for each i an $(n-2 \times n-2)$-minor P_i of N_i such that $\gcd(\det(P_i), i = 1, \dots, t) = 1$.

We begin by showing that $\Phi(G(n, a, b))$ can be generated by at most two elements. Let $0 < a \leq n$, and let $G(n, a)$ denote the graph obtained from K_n by removing the edges of a path on a vertices. The 'cyclicity' in our next lemma was first observed computationally by G. Michael Guy.

Lemma 5.5. *The group $\Phi(G(n, n-1))$ is cyclic of order $|h_{n-1}(2-n)|$. The group $\Phi(G(n, n))$ is cyclic of order $|h_n(2-n)|/n$.*

Proof. Let us write $\{1,\dots,n\}$ for the vertices of $G(n,n-1)$, and (i,j) for an edge linking the vertex i to the vertex j. Without loss of generality, we may enumerate the edges removed from K_n to get $G(n,n-1)$ as $(1,2)$, $(2,3)$, $\dots$, $(n-2,n-1)$. Consider the matrix M' obtained from the Laplacian M of $G(n,n-1)$ by subtracting the last row of M to each of the other rows. Consider now the $(n-2\times n-2)$-minor M'' of M' obtained by removing the first and last columns of M', and the last two rows of M'. It is easy to verify that $\det(M'')=1$. Thus, the greatest common divisor of the determinants of the $(n-2\times n-2)$-minors of M is 1, and $\Phi(G(n,n-1))$ is cyclic.

Let J_n denote the $(n\times n)$-matrix all of whose entries are 1. Recall that $\kappa(G)=\det(J_n+M)/n^2$ ([5], 6.4). The complexity of $G(n,n-1)$ is easily computed using this formula.

In the case of $G(n,n)$, we proceed similarly. The edges removed from K_n are now $(1,2)$, $(2,3)$, $\dots$, $(n-1,n)$. Consider the matrix M' obtained from the Laplacian M of $G(n,n)$ by subtracting the last row of M to each of the other rows. Consider now the $(n-2\times n-2)$-minor M'' of M' obtained by removing the last two columns of M', and the first and last rows of M'. It is easy to verify that $\det(M'')=1$. □

Remark 5.6 An explicit formula for the coefficients of $(-1)^{a-1}h_a(2-n)$ can be deduced from Corollary VIII in [32].

Let us write $\{1,\dots,n\}$ for the vertices of $G(n,a,b)$. Without loss of generality, we may enumerate the $n-3$ edges removed from the complete graph to get $G(n,a,b)$ as $(1,2)$, $(2,3)$, $\dots$, $(a-1,a)$ (for the path on a vertices) and $(a+1,a+2)$, $(a+2,a+3)$, $\dots$, $(n-2,n-1)$ (for the path on $b=n-1-a$ vertices). To prove that $\Phi(G(n,a,b))$ can be generated by two elements, we note that removing the edge $(a,a+1)$ from $G(n,a,b)$ results in the graph $G(n,n-1)$ which is cyclic by the previous lemma. Our claim that $\Phi(G(n,a,b))$ can be generated by two elements follows then from 5.1. The order of $\Phi(G(n,a,b))$ is computed using the formula $\kappa(G)=\det(J_n+M)/n^2$ ([5], 6.4).

Consider the matrix M' obtained from the Laplacian M of $G(n,a,b))$ by subtracting the last row of M to each of the other rows. For each integer $\ell=1,\dots,b+1$, consider now the $(n-2\times n-2)$-minor $M'[\ell]$ of M' obtained by removing the first and last columns of M', and by removing the a-th row and the $(a+\ell)$-th row. The minor $M'[\ell]$ is made of four blocks

$$\begin{pmatrix} A & 0 \\ B & N[\ell] \end{pmatrix},$$

where $\det(A)=1$, and $N[\ell]$ is by definition the matrix obtained from the $(b+1)\times b$-matrix N below by removing its ℓ-th row:

$$N:=\begin{pmatrix} n-1 & 1 & 0 & \dots & 0 \\ 1 & n-2 & 1 & & \vdots \\ 0 & 1 & \ddots & \ddots & 0 \\ \vdots & & \ddots & & 1 \\ 0 & \dots & 0 & 1 & n-1 \\ -1 & \dots & -1 & -1 & -1 \end{pmatrix}.$$

Consider the matrix N as having coefficients in $\mathbb{Z}[n]$, so that $\det(N[\ell])$ is a polynomial in the variable n. When $\ell=b+1$, we have $\det(N[b+1])=(-1)^b\mathrm{char}(D_b)(2-n)$.

We have thus found a matrix row and column equivalent to the Laplacian of $G(n,a,b)$ with an $(n-2\times n-2)$ minor whose determinant divides $\mathrm{char}(D_b)(2-n)$. Reversing the

roles played by a and b, we find that a matrix row and column equivalent to the Laplacian of $G(n,a,b)$ has an $(n-2\times n-2)$ minor whose determinant divides $\mathrm{char}(D_a)(2-n)$. It follows that γ divides the greatest common divisor of $\mathrm{char}(D_a)(2-n)$ and $\mathrm{char}(D_b)(2-n)$. Recall that $\mathrm{char}(D_a)(2-n)=(-n)h_a(2-n)$. Then γ divides $n\gcd(h_a(2-n),h_b(2-n))$.

Computations indicate, rather surprisingly, that for each $\ell=1,\dots,b$, we have $|\det(N[\ell])| = |h_b(2-n)|$. It would follows from this fact that $\gamma \mid \gcd(h_a(2-n),h_b(2-n))$. We prove this latter fact below without explicitly computing $|\det(N[\ell])|$.

Lemma 5.7. *Let p be a prime divisor of n. Then* $\det(N[b]) \equiv (-1)^b b \pmod p$.

Proof. Let $N[b]^*$ denote the comatrix of $N[b]$. We have

$$N[b]\,{}^t(1,\dots,1) = {}^t(n,\dots,n,-b).$$

Multiply both side of this equation by $N[b]^*$ to obtain

$${}^t(\det(N[b]),\dots,\det(N[b])) = N[b]^*\,{}^t(n,\dots,n,-b).$$

To evaluate the last entry of the right hand side modulo a prime p dividing n, it suffices to compute the determinant of the principal minor $N[b]^{b,b}$ obtained from $N[b]$ by removing its last row and column. We claim that $\det(N[b]^{b,b}) \equiv (-1)^{b-1} \pmod p$, from which the lemma follows. Consider the matrix modulo p:

$$N[b]^{b,b} \equiv \begin{pmatrix} -1 & 1 & 0 & \dots & 0 \\ 1 & -2 & 1 & & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & & 1 & -2 & 1 \\ 0 & \dots & 0 & 1 & -2 \end{pmatrix}.$$

Add the first column to the second, and then add the first row to the second. Continue this easy row and column reduction of this matrix to obtain that its determinant is $(-1)^{b-1}$.

It follows from the above discussion that we have obtained an $(n-2\times n-2)$ minor of a matrix row and column equivalent to M whose determinant is congruent to $(-1)^b b$ modulo any prime p dividing n. Reversing the roles played by a and b, we also obtain an $(n-2\times n-2)$ minor of a matrix row and column equivalent to M whose determinant is congruent to $(-1)^a a$ modulo any prime p dividing n. Thus there exists integers c and d such that $\gamma \mid c$ and $\gamma \mid d$, and $c \equiv (-1)^a a \pmod p$ and $d \equiv (-1)^b b \pmod p$. If $p \nmid a$, then $p \nmid \gamma$, as desired. If $p \mid a$ (and $p \mid n$), then $p \mid n-a$, with $n-a = b+1$. It follows that $p \nmid b$, so that $p \nmid \gamma$, as desired. We have thus shown that $\gamma \mid \gcd(h_a(2-n),h_b(2-n))$.

Lemma 5.8. *Assume that* $\gcd(a,b)=1$. *Then for any integer c,* $\gcd(h_a(c),h_b(c))=1$.

Proof. Let $\mathrm{Res}_x(h_a(x),h_b(x))$ denote the resultant of $h_a(x)$ and $h_b(x)$. Then there exist integer polynomials $\alpha(x)$ and $\beta(x)$ such that $\alpha(x)h_a(x)+\beta(x)h_b(x) = \mathrm{Res}_x(h_a(x),h_b(x))$. Thus, to prove our lemma, it suffices to show that $\mathrm{Res}_x(h_a(x),h_b(x)) = \pm 1$. The factorization of $h_a(x)$ and $h_b(x)$ is given explicitly in 5.2. Since $\gcd(a,b)=1$, these polynomials have no common factors. Since the resultant is multiplicative, we are reduced to proving that $\mathrm{Res}_x(f_a(x),f_b(x)) = \pm 1$ when $f_a(x)$ and $f_b(x)$ are any two irreducible factors in $\mathbb{Z}[x]$ of $h_a(x)$ and $h_b(x)$, respectively.

Given any integer polynomial $f_a(x)$, define

$$\phi_a(z) := z^{\deg(f_a(x))} f_a(z+1/z).$$

Let now $f_a(x)$ and $f_b(x)$ be two monic integer polynomials.

5.9 We claim that the prime divisors of $r := \mathrm{Res}_x(f_a(x), f_b(x))$ are also prime divisors of $R := \mathrm{Res}_z(\phi_a(z), \phi_b(z))$. Indeed, let $\alpha(z)$ and $\beta(z)$ be integer polynomials such that $\alpha(z)\phi_a(z) + \beta(z)\phi_b(z) = R$.

Consider now $\mathbb{Z}[z + 1/z]$ as a polynomial ring in the variable $z + 1/z$. This ring is in a natural way a subring of the ring $\mathbb{Z}[z, 1/z]$. The extension $\mathbb{Z}[z, 1/z]$ is integral over $\mathbb{Z}[z + 1/z]$, with basis $\{1, z\}$. The minimal polynomial of z over $\mathbb{Z}[z + 1/z]$ is $y^2 - (z + 1/z)y+1$. Thus, given any polynomial $\gamma(z)$ in $\mathbb{Z}[z]$, we can find polynomials $c_1(z+1/z)$ and $c_2(z+1/z)$ such that $\gamma(z) = c_1(z+1/z)+zc_2(z+1/z)$. In particular, we find $a_1(z+1/z)$ and $a_2(z + 1/z)$ in $\mathbb{Z}[z + 1/z]$ such that $\alpha(z)z^{\deg(f_a(x))} = a_1(z + 1/z) + za_2(z + 1/z)$. Similarly, we can write $\beta(z)z^{\deg(f_b(x))} = b_1(z + 1/z) + zb_2(z + 1/z)$ for some $b_1(z + 1/z)$ and $b_2(z + 1/z)$ in $\mathbb{Z}[z + 1/z]$. Hence, our relation

$$\alpha(z)z^{\deg(f_a(x))}f_a(z + 1/z) + \beta(z)z^{\deg(f_b(x))}f_b(z + 1/z) = R$$

implies the existence of an identity

$$a_1(z + 1/z)f_a(z + 1/z) + b_1(z + 1/z)f_b(z + 1/z) = R.$$

In other words, there exist integer polynomials $a_1(x)$ and $b_1(x)$ such that

$$a_1(x)f_a(x) + b_1(x)f_b(x) = R. \tag{4}$$

Let p be a prime divisor of r, and denote by a 'bar' the reduction modulo p. Since $f_a(x)$ and $f_b(x)$ are monic, $\bar{r}$ is the resultant of $\bar{f}_a(x)$ and $\bar{f}_b(x)$. Since $\bar{r} = 0$ in $\mathbb{Z}/p\mathbb{Z}$, $\bar{f}_a(x)$ and $\bar{f}_b(x)$ have a common root. Evaluating (4) at this common roots implies that $\bar{R} = 0$, as desired.

To conclude the proof of Lemma 5.8, we need to compute the resultant of the minimal polynomial $f_{2a,s}(x)$ of $\xi_{2a}^s + \xi_{2a}^{-s}$, $s = 1, \ldots, a - 1$, and the minimal polynomial $f_{2b,t}(x)$ of $\xi_{2b}^t + \xi_{2b}^{-t}$, $t = 1, \ldots, b - 1$. Note that since we assume $\gcd(a, b) = 1$, we may assume that a is odd. Then $\xi_{2a} = -\xi_a$, and $f_{2a,s}(x) = \pm f_{a,s}(-x)$. If both a and b are odd, we find that $\mathrm{Res}(f_{2a,s}(x), f_{2b,t}(x)) = \pm\mathrm{Res}(f_{a,s}(x), f_{b,t}(x))$, since $\mathrm{Res}(f(x), g(x)) = \pm\mathrm{Res}(f(-x), g(-x))$. If b is even, then $-\xi_{2b}$ is also a primitive $2b$-th root of 1, and thus a conjugate of ξ_{2b}. So when $t = 2r$ is even, $f_{2b,t}(x) = f_{b,r}(x)$, and when t is odd, $f_{2b,t}(x) = f_{2b,t}(-x)$. We find that we only need to show that $\mathrm{Res}(f_{a,1}(x), f_{b,1}(x)) = \pm1$ for any $a, b > 1$ with $\gcd(a, b) = 1$. This is done in the next lemma.

Lemma 5.10. *Let $f_a(x)$ denote the minimal polynomial over the integers of $\xi_a + \xi_a^{-1}$. Assume that $a, b > 1$ and $\gcd(a, b) = 1$. Then $\mathrm{Res}_x(f_a(x), f_b(x)) = \pm1$.*

Proof. Assume $a > 2$. We claim that $\phi_a(z) := z^{\deg(f_a(x))}f_a(z + 1/z)$ is the minimal polynomial over $\mathbb{Z}$ of ξ_a. Indeed, since $\xi_a + \xi_a^{-1}$ is a real number and ξ_a is not, and since $\mathbb{Q}(\xi_a + \xi_a^{-1}) \subset \mathbb{Q}(\xi_a)$, we find that the degree of $\phi_a(z)$ is equal to $[\mathbb{Q}(\xi_a) : \mathbb{Q}]$. Since ξ_a is a root of $\phi_a(z)$, $\phi_a(z)$ is the minimal polynomial. The assertion $\mathrm{Res}_x(f_a(x), f_b(x)) = \pm1$ when both $a, b > 1$ follows now from 5.9 and from the assertion $\mathrm{Res}_z(\phi_a(z), \phi_b(z)) = 1$, proved in [1] or [20] when $\gcd(a, b) = 1$ and $a, b > 1$. When $a = 2$, $f_a(x) = x - 2$, and $\phi_a(z) = (z + 1)^2$. Thus, $\mathrm{Res}_z(\phi_a(z), \phi_b(z)) = \mathrm{Res}_z(z + 1, \phi_b(z))^2$, and we obtain the desired result again from [1]. □

This concludes the proof of Proposition 5.4.

Remark 5.11 Let $\varphi(x)$ denote Euler's totient function. For a fixed n, the proportion of graphs $G(n, a, b)$ with $a, b > 1$ and $\Phi(G(n, a, b))$ cyclic is at least $\frac{\varphi(n-1)-2}{n-4}$ if $n \geq 6$ is even, or $\frac{\varphi(n-1)-2}{n-3}$ if $n \geq 5$ is odd. Indeed, $\gcd(a, b) = 1$ and $a + b = n - 1$ occur simultaneously if and only if a is coprime to $n - 1$.

Consider now the proportion of graphs $G(i,a,b)$ with $i \leq n$ whose group $\Phi(G(i,a,b))$ is cyclic. This proportion is at least

$$\frac{\sum_{i=4}^{n-1} \varphi(i) - 2}{g(n)},$$

where $g(n)$ is a polynomial of degree 2 in n, with leading coefficient $1/2$. It is well known that

$$\frac{1}{n^2}\sum_{i=1}^{n} \varphi(i) = \frac{3}{\pi^2} + \mathcal{O}(\frac{\log(n)}{n}).$$

Hence, we find that among all graphs $G(n,a,b)$, the proportion of graphs having a cyclic group $\Phi(G(n,a,b))$ is at least

$$\lim_{n\to\infty} \frac{\sum_{i=1}^{n} \varphi(i)}{n^2/2} = \frac{6}{\pi^2}.$$

Let a, b, and n be positive integers such that $a+b=n$. Let $H(n,a,b)$ denote the graph obtained by removing from K_n the $n-2$ edges of two vertex-disjoint paths on a and b vertices, respectively. The following statement was first observed computationally by G. Michael Guy when n is prime.

Proposition 5.12. *Let $a, b \geq 2$ be such that $a+b=n$. Then*

$$\Phi(H(n,a,b)) = \mathbb{Z}/\gamma\mathbb{Z} \times \mathbb{Z}/\delta\mathbb{Z},$$

with $\gamma \mid \delta$ and $\gamma\delta = |h_a(2-n)h_b(2-n)|$. Moreover, γ divides $\gcd(|h_a(2-n)|, |h_b(2-n)|)$. When $\gcd(a,b)=1$, $\Phi(H(n,a,b))$ is cyclic.

Proof. This proposition is proved using the same techniques as in the proof of 5.4. The details are left to the reader. An alternate proof of the fact that when $\gcd(a,b)=1$, $\Phi(H(n,a,b))$ is cyclic, is as follows. Note that by removing the edge $(a, a+1)$ from $H(n,a,b)$, we obtain the graph $G(n,n)$, with $\Phi(G(n,n))$ of order $|h_n(2-n)|/n$. When $\gcd(a,b)=1$ and $a+b=n$, $\gcd(a,n)=\gcd(b,n)=1$. If follows from 5.8 that $|\Phi(H(n,a,b))|$ and $|\Phi(G(n,n))|$ are coprime, so $\Phi(H(n,a,b))$ is cyclic by 6.1. □

Remark 5.13 Let $\{1,\ldots,n\}$ denote the vertices of K_n, and let $(1,2),\ldots,(a-1,a)$ denote the edges removed from K_n to obtain $G(n,a)$. Let $G^c(n,a)$ denote the graph obtained from $G(n,a)$ by removing the edge $(1,a)$. The graph $G^c(n,a)$ is thus obtained from the complete graph K_n by removing a cycle on a vertices. Lemma 5.5 and 5.1 imply that the groups of $G^c(n,n-1)$ and $G^c(n,n)$ are either cyclic or are generated by two elements. Computations seem to indicate that these groups are never cyclic. In fact, the order of $\Phi(G^c(n,n-1))$ is a perfect square s^2 when n is even (use [5], 6.4, and the spectrum of the cycle in [5], page 17), and computations provide evidence that $\Phi(G^c(n,n-1)) = (\mathbb{Z}/s\mathbb{Z})^2$.

6. Adding chains

We present in this section a construction of graphs with cyclic groups $\Phi(G)$.

6.1 Recall the following facts. Let v and v' be two vertices of G linked by $c>0$ edges. Let G_1 denote the graph obtained from G by removing these c edges, and let G_2 denote the graph obtained from G_1 by identifying v with v'. We will always assume in the rest of this section that the resulting graph G_1 is connected. Then $|\Phi(G)| = |\Phi(G_1)| + c|\Phi(G_2)|$. Let $\phi_1 := |\Phi(G_1)|$ and $\phi_2 := |\Phi(G_2)|$. We showed in [27], 5.1, that if $\gcd(\phi_1,\phi_2)=1$ or, equivalently, if $\gcd(\phi_1, |\Phi(G)|)=1$, then $\Phi(G)$ is cyclic. The proof is easy, and we review it in the context of the next lemma.

Lemma 6.2. *Suppose that* $\gcd(|\Phi(G)|, \phi_1) = 1$. *Then* $\Phi(G)$ *and* $\Phi(G_1)$ *are cyclic.*

Proof. Let M denote the Laplacian of G. Assume that the edges to be removed are between v_1 and v_2. Then the $(n-2 \times n-2)$-minor $M^{2,2}$ of M obtained by removing the first two rows and the first two columns is also an $(n-2 \times n-2)$-minor of the Laplacian of G_1. Suppose that $\Phi(G_1)$ is not cyclic. Then there exists a prime p that divides both ϕ_1 and $\det(M^{2,2})$. But it can easily be checked that $|\det(M^{2,2})| = \phi_2$. It follows that p also divides $|\Phi(G)| = \phi_1 + c\phi_2$, a contradiction. The proof for $\Phi(G)$ is similar. □

Example 6.3 Obviously, any graph without vertices of degree 1 and with $|\Phi(G)|$ prime has the property that $\gcd(\phi_1, |\Phi(G)|) = 1$ for any pair of adjacent vertices with G_1 connected. Thus, if $|\Phi(G)|$ is prime, all the subgraphs of G of the form G_1 have $\Phi(G_1)$ cyclic.

Remark 6.4 It is not true that if $\Phi(G)$ is cyclic, then there exists a pair of adjacent vertices v and v' in G such that $\gcd(\phi_1, |\Phi(G)|) = 1$. Indeed, consider the graph G obtained by gluing together a vertex of a cycle of length $a > 1$ with a vertex of a cycle of length $b > 1$, with $\gcd(a, b) = 1$. Then $\Phi(G) = \mathbb{Z}/ab\mathbb{Z}$ is cyclic, but for any edge of G, $\Phi(G_1)$ is cyclic of order either a or b.

It is not true that if $\Phi(G)$ is cyclic, then there exists a pair of adjacent vertices v and v' in G such that $\Phi(G_1)$ is cyclic. The following matrix A is the adjacency matrix of a connected graph G on 8 vertices with $\Phi(G)$ is cyclic (of squarefree order $42 \cdot 11$), and such that the group $\Phi(G_1)$ of every subgraph of G of the form G_1 is *not cyclic*. This graph was found by Grant Fiddyment after an exhaustive search:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Let G be a graph, and fix a pair of vertices $\{v, v'\}$ of G. Take $\nu \geq 3$ vertices $w_1, \ldots, w_\nu$, and link w_i to w_{i+1} by one edge for all $i \in \{1, \ldots, \nu - 1\}$, except that for one index i_0, the vertex w_{i_0} is linked to w_{i_0+1} by $d > 0$ edges. Let $G' = G'(\nu, d, i_0)$ denote the graph obtained from G by gluing the vertex w_1 to v and the vertex w_ν to v'. We say that the graph G' is obtained from G by *attaching, or adding, a chain at* v *and* v'.

Suppose that v and v' are linked by a single edge. We say that the graph G'' is obtained from G by *dividing the edge in* ℓ if G'' is simply the graph G with $\ell - 1$ new vertices on the original edge between v and v'. Our next proposition shows that starting with certain graphs G with $\Phi(G)$ cyclic, we can inductively construct infinitely many sequences of new cyclic graphs by attaching chains or dividing edges.

Proposition 6.5. *Let* G *be a graph with two fixed vertices* v *and* v' *linked by* $c > 0$ *edges as above, such that* $\phi_1 := |\Phi(G_1)|$ *and* $\phi_2 := |\Phi(G_2)|$ *are coprime, so that* $\Phi(G)$ *is cyclic.*

(a) *Let* $G' = G'(\nu, d, i_0)$ *be a graph obtained from* G *by attaching a chain at* v *and* v'. *Then* $\Phi(G')$ *is cyclic. More precisely, let* G'_1 *denote the graph obtained from* G' *by removing the* d *edges between* w_{i_0} *and* w_{i_0+1}. *Let* G'_2 *denote the graph obtained from* G'_1 *by identifying* w_{i_0} *and* w_{i_0+1}. *Then* $|\Phi(G'_1)| = \phi_1 + c\phi_2$ *and* $|\Phi(G'_2)| = (\nu-1)(\phi_1+c\phi_2)+\phi_2$ *are coprime,*

(b) *Assume that $c = 1$. Let G'' denote any graph obtained by dividing the edge between v and v'. Then $\Phi(G'')$ is cyclic.*

Proof. (a) We leave it to the reader to check that $|\Phi(G'_2)| = (\nu - 1)(\phi_1 + c\phi_2) + \phi_2$, using several times the deletion/contraction formula recalled in 6.1. If $|\Phi(G'_1)|$ and $|\Phi(G'_2)|$ are divisible by a prime p, then $p \mid \phi_2$ and, hence, $p \mid \phi_1$, since $p \mid \phi_1 + c\phi_2$. This contradicts the fact that ϕ_1 and ϕ_2 are coprime. We conclude that $\Phi(G')$ is cyclic using 6.1.

(b) Let G''_1 denote the graph obtained from G'' by removing one of the 'new' ℓ edges between v and v'. It is clear that $|\Phi(G''_1)| = \phi_1$. The associated graph G''_2 has $|\Phi(G''_2)| = \ell\phi_1 + \phi_2$. Clearly, if $\gcd(\phi_1, \phi_2) = 1$, then $\gcd(\phi_1, \ell\phi_1 + \phi_2) = 1$. We conclude using 6.1. □

Example 6.6 We can use the above proposition starting with any cycle G on $n > 2$ vertices and any pair $\{v, v'\}$ of adjacent vertices on the cycle. Indeed, removing an edge from G gives a tree G_1 with $|\Phi(G_1)| = 1$, and G_2 is a cycle on $n - 1$ vertices, so that $\gcd(\phi_1, \phi_2) = 1$.

Similarly, we can start with a 'modified' cycle having $c > 1$ edges between v and v'. Adding chains repeatedly to this graph and its successors produces a graph G which can also be described as in the corollary below. The proof of the corollary is an easy consequence of the proposition. A very similar statement is proved in [10], 2.6.

Corollary 6.7. *Start with a cycle, whose vertices and edges lie on a circle in the plane. Number the vertices as $v_1, \ldots, v_n$, with v_i linked to v_{i+1} for $i = 1, \ldots, n-1$, and v_n linked to v_1. Choose $d > 1$ and draw any number of edges between pairs of vertices of the cycle having one vertex in $\{v_2, \ldots, v_d\}$ and the other in $\{v_{d+2}, \ldots, v_n\}$, so long as all these edges are contained inside the circle and the resulting graph G is planar as drawn. Then $\Phi(G)$ is cyclic.*

Remark 6.8 We can use the above proposition and Example 6.6 to give upper bounds for the number of generators of certain groups $\Phi(G)$. For instance, take any cycle on n vertices, add one vertex w, and link (with one edge) this vertex to some vertices of the cycle. Call G the resulting graph. In the case where w is linked to all vertices of the cycle, the resulting graph G is a wheel, and the group of a wheel is known to be the product of two cyclic groups when n is odd ([6], 9.2). Removing from G any edge belonging to the initial 'rim' cycle produces a graph G_1 which can be built inductively from a smaller cycle by adding chains, as in Example 6.6, and then adding possibly up to two branches (trees with maximal degree 2). Thus, $\Phi(G_1)$ is cyclic, and 5.1 shows that $\Phi(G)$ *is generated by (at most) two elements.*

Take now two distinct cycles on n and n' vertices, with vertices $v_1, \ldots, v_n$ and $w_1, \ldots, w_{n'}$. Orient both cycles clockwise, and number the vertices of each cycle consecutively. Pick $s \geq 2$ indices $1 \leq i_1 < \cdots < i_s \leq n$ and s indices $1 \leq j_1 < \cdots < j_s \leq n'$. Let G denote the graph obtained from the disjoint union of the two cycles by linking v_{i_ℓ} to w_{j_ℓ} by one edge, for $\ell = 1, \ldots, s$. *The group $\Phi(G)$ is generated by (at most) three elements.* Indeed, removing one edge of the path between v_{i_1} and v_{i_2} on the first cycle and removing one edge of the path between w_{j_1} and w_{j_2} on the other cycle results in a graph G' which can be built inductively from a smaller cycle by adding chains as in 6.6, and then adding possibly some branches. Thus $\Phi(G')$ is cyclic, and we conclude using 5.1. In the case $n = n' = s$, the resulting graph is considered in [17], where the group $\Phi(G)$ is shown never to be cyclic, and to require three generators for certain n.

References

[1] T. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. **24** (1970), 457–462.

[2] S. Arno, M. Robinson, and F. Wheeler, *On denominators of algebraic numbers and integer polynomials*, J. Number Theory **57** (1996), 292–302.

[3] R. Bacher, P. de la Harpe and T. Nagnibeda, *The lattice of integral flows and the lattice of integral cuts on a finite graph*, Bull. Soc. Math. France **125** (1997), 167–198.

[4] K. Berman, *Bicycles and spanning trees*, SIAM J. Algebraic Discrete Methods **7** (1986), 1-12,

[5] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, 1974.

[6] N. Biggs, *Chip-firing and the critical group of a graph*, J. Algebr. Comb. **9** (1999), 25–46.

[7] N. Biggs, *The critical group from a cryptographic perspective*, Bull. London Math. Soc. **39** (2007), 829-836.

[8] J. Borwein and K. Choi, *On the representations of* $xy + yz + zx$, Experiment. Math. **9** (2000), no. 1, 153–158.

[9] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[10] S. Busonero, M. Melo, and L. Stoppino, *Combinatorial aspects of nodal curves*, Le Matematiche, vol. LXI (2006), Fascicolo I, pp. 109-141.

[11] S. Chen and S.K. Ye, *Critical groups for homeomorphism classes of graphs*, Discr. Math (2008), in press.

[12] A. Chiodo, *Quantitative Néron theory for torsion bundles*, arXiv:math/0603689v2, Preprint 2007.

[13] S. Chowla, *An extension of Heilbronn's class number theorem*, Quat. J. Math. **5** (1934), 304-307.

[14] H. Christianson and V. Reiner, *The critical group of a threshold graph*, Linear Algebra Appl. **349** (2002), 233–244.

[15] R. Cori and D. Rossin, *On the sandpile group of dual graphs*, European J. Combin. **21** (2000), no. 4, 447–459.

[16] E. van Dam, and W. Haemers, *Graphs with constant* μ *and* $\overline{\mu}$, Graph theory (Lake Bled, 1995), Discrete Math. **182** (1998), no. 1-3, 293–307.

[17] A. Dartois, F. Fiorenzi, and P. Francini, *Sandpile group on the graph* D_n *of the dihedral group*, European J. Combin. **24** (2003), no. 7, 815–824.

[18] K. Das, *The Laplacian spectrum of a graph*, Comput. Math. Appl. **48** (2004), no. 5-6, 715–724.

[19] D. Dhar, *Self-organized critical state of sandpile automaton models*, Phys. Rev. Lett. **64** (1990), no. 14, 1613–1616.

[20] F.-E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Hansischen Univ. **13** (1940), 357–412.

[21] C. Godsil and G. Royle, *Algebraic graph theory*, Graduate Texts in Mathematics **207**, Springer-Verlag, New York, 2001.

[22] R. Grone, R. Merris, and V. Sunder, *The Laplacian spectrum of a graph*, SIAM J. Matrix Anal. Appl. **11** (1990), no. 2, 218–238.

[23] Y. Hou, C. Woo, and P. Chen, *On the sandpile group of the square cycle* C_n^2, Linear Algebra Appl. **418** (2006), 457–467.

[24] B. Jacobson, A. Niedermaier, and V. Reiner, *Critical groups for complete multipartite graphs and Cartesian products of complete graphs*, J. Graph Theory **44** (2003), 231–250.

[25] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. reine angew. Math. **53** (1857), 173-175.

[26] M. Lien and W. Watkins, *Dual graphs and knot invariants*, Linear Algebra Appl. **306** (2000), 123–130.

[27] D. Lorenzini, *Arithmetical graphs*, Math. Ann. **285** (1989), no. 3, 481–501.

[28] D. Lorenzini, *A finite group attached to the Laplacian of a graph*, Discrete Math. **91** (1991), no. 3, 277–282.

[29] D. Lorenzini, *Arithmetical properties of Laplacians of graphs*, Linear and Multilinear Algebra **47** (2000), 281–306.

[30] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics **9**, American Mathematical Society, 1996.

[31] B. McKay, *http://cs.anu.edu.au/~bdm/data/graphs.html*

[32] J. Moon, *Enumerating labelled trees*, Graph Theory and Theoretical Physics, 261-272, Academic Press, 1967.

[33] M. Newman and R. Thompson, *Matrices over rings of algebraic integers*, Linear Algebra Appl. **145** (1991), 1–20.
[34] M. Raynaud, *Spécialisation du foncteur de Picard*, Inst. Hautes Études Sci. Publ. Math. **38** (1970), 27–76.
[35] J. Rushanan, *Combinatorial applications of the Smith normal form*, Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989). Congr. Numer. **73** (1990), 249–254.
[36] J. Rushanan, *Eigenvalues and the Smith normal form*, Linear Algebra Appl. **216** (1995), 177–184.
[37] E. Spence, *http://www.maths.gla.ac.uk/~es/*.
[38] E. Toumpakari, *On the sandpile group of regular trees*, European J. Combin. **28** (2007), no. 3, 822–842.
[39] P. Yuan, *Positive integer solutions of the equation* $xy+yz+zx=n$ (Chinese), Acta Math. Sinica (Chin. Ser.) **43** (2000), no. 3, 391–398.

D.L. was supported by NSA Grant H98230.

Dino Lorenzini, Department of Mathematics,
University of Georgia, Athens, GA 30602, USA.