Number theory

We work over finite extensions of $\mathbb{Q}$.

A number α in $\mathbb{C}$ is an algebraic integer if it is a root of a monic polynomial in $\mathbb{Z}[t]$. It is an algebraic number if it is a root of a polynomial in $\mathbb{Z}[t]$

example: any graph eigenvalue is an algebraic integer

Question: which algebraic integers are graph eigenvalues?

Field theory Suppose the field $\mathbb{E}$ is an extension of degree d over the field $\mathbb{F}$. Then $\mathbb{E}$ is a vector space of dimension d over $\mathbb{F}$.

If $\lambda \in \mathbb{E}$ and M_λ is the linear map multiplication, then M_λ can be represented by a $d \times d$ matrix. Hence $\mathbb{E}$ can be viewed as a subalgebra of $\mathrm{Mat}_{d \times d}(\mathbb{F})$.

Number theorists call the trace of M_λ the trace of λ, and they call the determinant the norm.

example $$\mathbb{C} \cong \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$$

Henceforth $\mathbb{F} = \mathbb{Q}$, and we work with finite extensions of $\mathbb{Q}$, viewed as subfields of $\mathbb{C}$. If $|\mathbb{E} : \mathbb{Q}|$ is finite and $\lambda \in \mathbb{E}$, then there is a least positive integer d such that $1, \ldots, \lambda^{d-1}$ are linearly independent and λ^d lies in their span.

Algebraic integers (& numbers)

An algebraic integer is a complex number that satisfies a monic polynomial with only integer coefficients.

Lemma. A complex number is an algebraic integer if & only if it an eigenvalue of a integer matrix.

Proof If A is an integer matrix, each eigenvalue satisfies the minimal polynomial of A.

So assume λ satisfies a monic polynomial f of degree d with only integer coefficients

Then $\mathrm{span}\{1, \dots, \lambda^{d-1}\}$ is a subspace, invariant under M_λ. The matrix representing M_λ on this subspace is the companion matrix of ψ, and has only integer coefficients.

product	eigenvalues
$A \otimes B$	$\lambda_r \mu_s$
$A \otimes I + I \otimes B$	$\lambda_r + \mu_s$
$A \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\pm \lambda_r$

Theorem The algebraic integers form a ring. $\square$

An **algebraic number** is a complex number that satisfies a polynomial in $\mathbb{Q}[t]$, equivalently a polynomial with only integer coefficients.

Exercises

(1) If λ is an algebraic number, there is an integer m such that $m\lambda$ is an algebraic integer

(2) If λ is a algebraic number, so is λ^{-1} — the algebraic numbers form a field.

(3) The eigenvalues of the following families of graphs form rings

(a) all graphs (b) all regular graphs

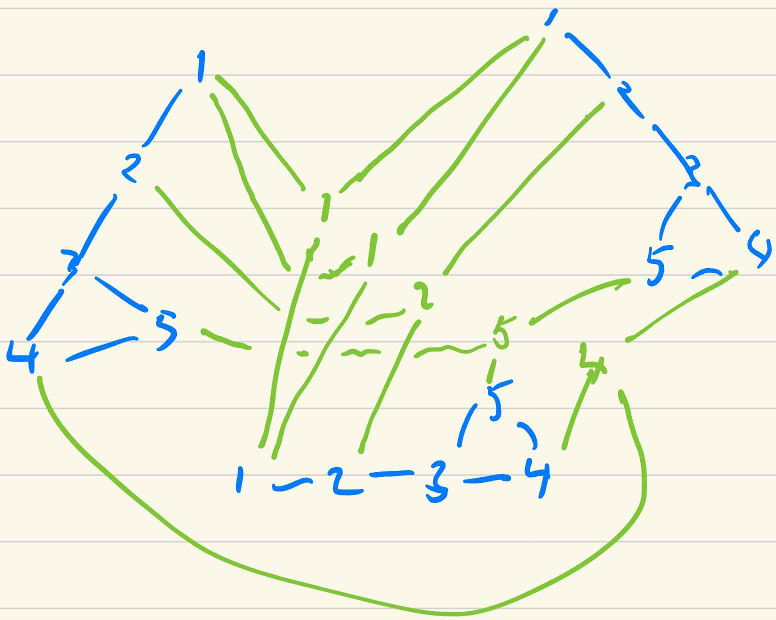
(c) all Cayley graphs (d) all arc-transitive graphs

(4) The set of all spectral radii of graphs is closed under addition & multiplication

If ψ is the minimal polynomial over $\mathbb{Q}$ of the algebraic integer λ, then ψ is irreducible and $\mathbb{Q}[t]/(\psi(t))$ is a field ($\mathbb{Q}(\lambda)$, in fact)

An algebraic integer μ is conjugate to an algebraic integer λ if it is a root of the minimal polynomial of λ.

Theorem If X is a graph, there is a Cayley graph Z such that $\phi(X,t) \mid \phi(Z,t)$.



$$\begin{bmatrix} 0 & B & B & B \\ B^T & A & 0 & 0 \\ B^T & 0 & A & 0 \\ B^T & 0 & 0 & A \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ x \\ -x \end{bmatrix}$$

Theorem. If X has a 1-factorization, then there is a Cayley graph Y such that $\phi(X,t) \mid \phi(Y,t)$.

Proof If $A = A(X)$ and X admits a 1-factorization then

$$A = P_1 + \cdots + P_d$$

where $P_1, \ldots, P_d$ are the adjacency matrices of 1-factors. So they are permutation matrices and generate a permutation group Γ.

Let Y be the Cayley graph $Y = X(\Gamma, \{P_1, \ldots, P_d\})$

could have $n!$ vertices ($n = |V(X)|$)

Each matrix P_i maps to a permutation Q_i in the regular representation of Γ. This map is an isomorphism. The sum $B = Q_1 + \cdots + Q_d$ is the adjacency matrix of the Cayley graph Y.

The maps $Q_i \mapsto P_i$ extends to an algebra homomorphism, and it follows that $\phi(X,t)$ divides $\phi(Y,t)$.

What if X does not have a 1-factorization?

Well, X is regular and so $X \times K_2$ is bipartite & regular. Hence it has a 1-factorization.

(The eigenvalues of $X \times K_2$ are $\pm\theta$, where θ runs over the eigenvalues of X.)

Theorem Every Laplacian eigenvalue is a graph eigenvalue.

Proof

Step 1: convert to a non-negative matrix

Assume $L = \Delta - A$. Define

$$\tilde{L} := \Delta \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + A \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

This has characteristic polynomial $\phi(\Delta+A, t)\,\phi(\Delta-A, t)$

Step 2: convert to a 01-matrix.

Let k be the maximum degree of a vertex.

Suppose we have 01-matrices $M_0, \dots, M_k$ of order $\ell \times \ell$ such that

(a) $M_0 = 0$,

(b) $\mathrm{tr}(M_i) = 0$,

(c) $M_i \underset{\sim}{1} = i \underset{\sim}{1}$,

(d) all matrices $M_1, \dots, M_k, M_1^T, \dots, M_k^T$ commute.

How? Circulants!

Construct $\tilde{\tilde{L}}$ from $\tilde{L}$ by replacing entries $i \longmapsto M_i$.

Choose $l \times 1$ Z such that $Z^{-1} M_i Z$ is diagonal and $(Z^{-1} M_i Z) = i$. Then

$$\begin{pmatrix} Z^{-1} & & \\ & \ddots & \\ & & Z^{-1} \end{pmatrix} \tilde{\tilde{L}} \begin{pmatrix} Z & & \\ & \ddots & \\ & & Z \end{pmatrix}$$

is matrix of $l \times l$ blocks, each block diagonal. Therefore it is permutation equivalent to a block diagonal matrix with l blocks, one equal to L.