Example 1. Quadratic Extension

field	ring	prime ideal	finite field
$K=F(\sqrt{m})$	$O_K = \mathbb{Z}[\sqrt{m}]$	$\mathfrak{p} \supset pO_K$	$O_K / \mathfrak{p}$
|	|	|	|
$F=\mathbb{Q}$	$O_F=\mathbb{Z}$	$p\mathbb{Z}$	$\mathbb{Z} / p\mathbb{Z}$

g = # of such $\mathfrak{p}$, f = degree of $O_K / \mathfrak{p}$ over O_F / pO_F

$$\mathfrak{p}^e \supset pO_K \not\subset \mathfrak{p}^{e+1}$$

efg=2

Assume, m is a square-free integer congruent to 2 or 3 (mod 4).

A reference: H. Stark's article in From Number Theory to Physics, M. Waldschmidt et al (Eds.), Springer- Verlag, Berlin, 1992, pages 313-393.

Decomposition of Primes in Quadratic Extensions

3 CASES $K=F(\sqrt{m})/F$, $F=\mathbb{Q}$

1) **p inert:** f=2. pO_K = prime ideal in K, $m \not\equiv x^2 \pmod p$

2) **p splits:** g=2. $pO_K = \mathfrak{p}\,\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$, $m \equiv x^2 \pmod p$

3) **p ramifies:** e=2. $pO_K = \mathfrak{p}^2$, p divides 4m

Gal(K/F)={1,-1}

Frobenius automorphism
= Legendre Symbol =

$$\left(\frac{4m}{p}\right) = \begin{cases} -1, & \text{in case } 1 \\ 1, & \text{in case } 2 \\ 0, & \text{in case } 3 \end{cases}$$

p does not divide 4m implies p has 50% chance of being in Case 1 (and 50% chance of being in case 2)

Assume, m is a square-free integer ≡ 2 or 3 (mod 4).

Artin L-Functions

$K \supset F$ number fields with K/F Galois

$O_K \supset O_F$ rings of integers

$\mathfrak{P} \supset \mathfrak{p}$ prime ideals ($\mathfrak{p}$ unramified , i.e., $\mathfrak{p} \not\subset \mathfrak{P}^2$)

Frobenius Automorphism when $\mathfrak{p}$ is unramified.

$$\left(\frac{K/F}{\mathfrak{P}}\right) = \sigma_{\mathfrak{P}} \in Gal(K/F), \qquad \sigma_{\mathfrak{P}}(x) \equiv x^{|O_F/\mathfrak{p}|} \pmod{\mathfrak{P}}, \text{ for } x \in O_K$$

$\sigma_{\mathfrak{P}}$ induces generator of finite Galois group, $\mathrm{Gal}((O_K/\mathfrak{P})/(O_F/\mathfrak{p}))$
determined by $\mathfrak{p}$ up to conjugation if $\mathfrak{P}/\mathfrak{p}$ unramified
$f(\mathfrak{P}/\mathfrak{p})$ = order of $\sigma_{\mathfrak{P}} = [O_K/\mathfrak{P} : O_F/\mathfrak{p}]$
$g(\mathfrak{P}/\mathfrak{p})$=number of primes of K dividing $\mathfrak{p}$

Artin L-Function for $s \in \mathbb{C}$, π a representation of Gal(K/F).
Give only the formula for unramified primes $\mathfrak{p}$ of F.
Pick $\mathfrak{P}$ a prime in O_K dividing $\mathfrak{p}$.

$$L(s,\pi) \text{"="} \prod_{\mathfrak{p}} \det\left(1 - \pi\left(\frac{K/F}{\mathfrak{P}}\right) N\mathfrak{p}^{-s}\right)^{-1}$$

Chebotarev Density Theorem

For a set S of primes of F, define the analytic density of S.

$$\delta(S)=\lim_{s\to 1+}\left(\frac{\sum_{p\in S} p^{-s}}{-\log(s-1)}\right)$$

Theorem. Set C(p)=the conjugacy class of the Frobenius automorphism of prime ideals $\mathfrak{P}$ of K above p. Then, for every conjugacy class C in G=Gal(K/F),

$$\delta\{p \mid C(p)=C\}=\frac{|C|}{|G|}.$$

The proof requires the facts that L(s,π) continues to s=1 with no pole or zero if π≠1, while L(s,1)=ζ_F(s) has a simple pole at s=1 .

Graph Galois Theory

Graph Y an unramified covering of Graph X means (assuming no loops or multiple edges)

∃ π:Y→X is an onto graph map such that for every x∈X & for every y ∈ π^{-1}(x),

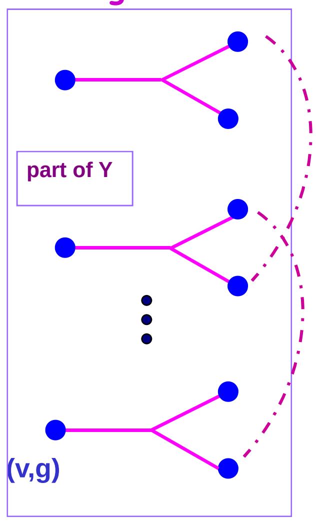
π maps the points z ∈ Y adjacent to y 1-1, onto the points w ∈ X adjacent to x.

Normal d-sheeted Covering means:
∃ d graph isomorphisms g_1 ,..., g_d mapping Y → Y
such that π g_j (y) = π (y) ∀ y ∈ Y
The Galois group G(Y/X) = { g_1 ,..., g_d }.

This is an analog of coverings of manifolds, Riemann surfaces, etc.

How to Create a Galois Covering

First pick a spanning tree T_X in X (no cycles, connected, includes all vertices of X).



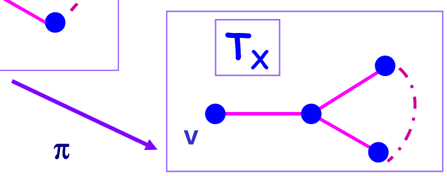
Second make n=|G| copies of the tree T_X in X. These are the sheets of Y. Label the sheets with $g \in G$. The vertices of Y are (x,g) for x vertex of X, $g \in G$.

G action on Y:

on sheets: g(sheet h) = sheet(gh)

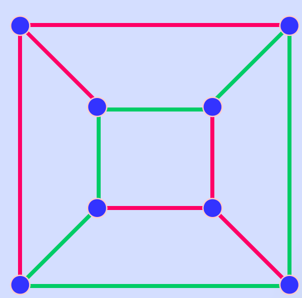
on vertices: g(x,h)=(x,gh)

on paths: g(path from (v,h) to (w,j)) = path from (v,gh) to (w,gj)

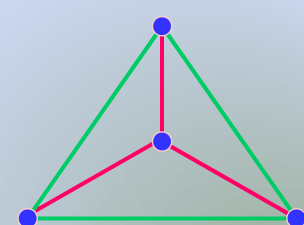


Given G, get examples Y by giving permutation representation of generators of G to lift edges of X left out of T_X.

Example 1. Quadratic Cover

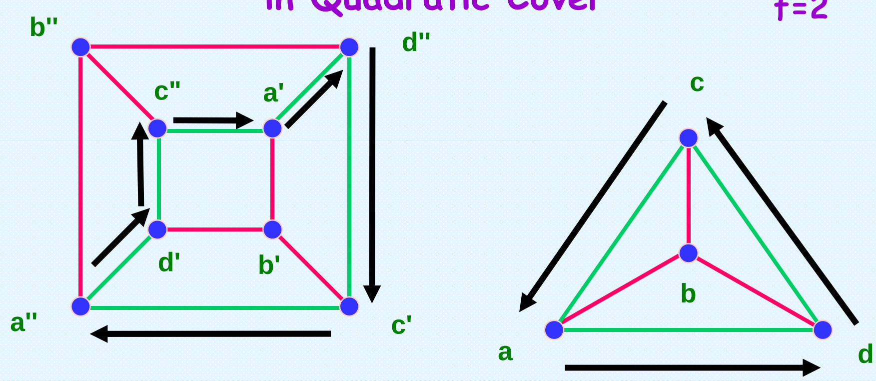


Cube covers Tetrahedron



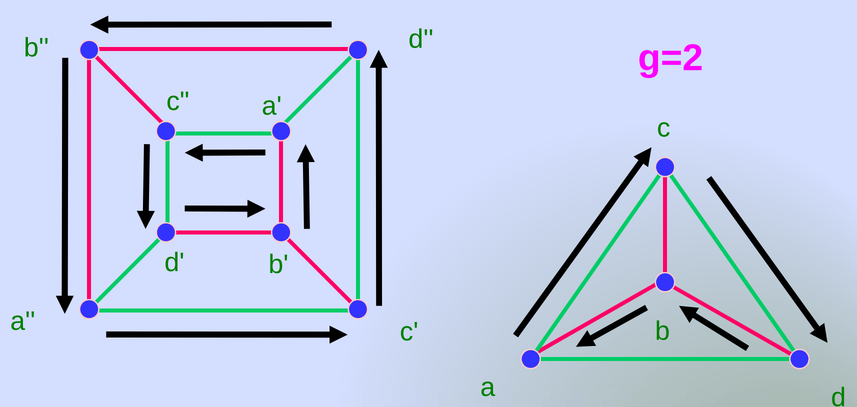
Spanning Tree in X is red.
Corresponding sheets of Y are also red

Example of Splitting of Primes in Quadratic Cover



Picture of Splitting of Prime which is inert; i.e., **f=2, g=1, e=1**
1 prime cycle D above, & D is lift of C^2.

Example of Splitting of Primes in Quadratic Cover



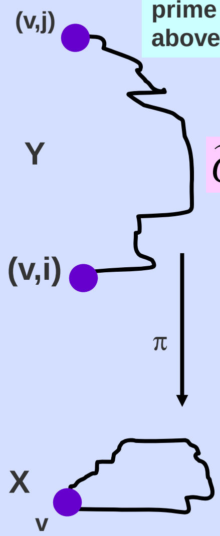
Picture of Splitting of Prime which splits completely; i.e., f=1, g=2, e=1
2 primes cycles above

Frobenius Automorphism

D a prime above C

$$\text{Frob}(D) = \left(\frac{Y/X}{D}\right) = ji^{-1} \in G = \text{Gal}(Y/X)$$

where ji^{-1} maps sheet i to sheet j



$\widetilde{C}$ = the unique lift of C in Y starting at (v,i) ending at (v,j)

C = path in X

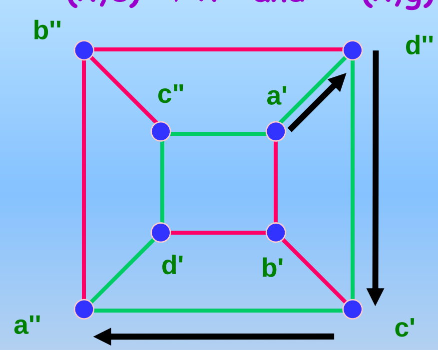
$\widetilde{C}$ is not necessarily closed

$$length(\widetilde{C}) = length(C)$$

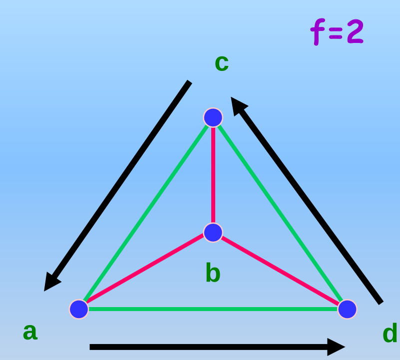
(D a prime above C is closed and is obtained by f liftings like $\widetilde{C}$)

Exercise: Compute Frob(D) on preceding pages, G={e,g}.

Galois Group={e,g}: Label cube vertices (x,e) → x' and (x,g) → x'', x in K_4



Y=cube



X=K_4

Frobenius of prime in X = non-trivial element of Galois group
since
if we lift path on X once, we get to the other sheet of the cover

Properties of Frobenius

1) Replace (v,i) with (v,hi). Then Frob(D) = ji^{-1} is replaced with $hji^{-1}h^{-1}$. Or replace D with different prime above C and see that
   Conjugacy class of Frob(D) $\in$ Gal(Y/X) unchanged.
2) Varying start vertex v of C in X does not change Frob(D).
3) $\mathrm{Frob}(D)^j = \mathrm{Frob}(D^j)$.

Artin L-Function

ρ = representation of G=Gal(Y/X), $u \in \mathbb{C}$, |u| small

$$L(u,\rho,Y/X) = \prod_{[C]} \det\left(1 - \rho\left(\frac{Y/X}{D}\right) u^{\nu(C)}\right)^{-1}$$

[C]=equivalence class of primes of X
$\nu(C)$=length C, D a prime in Y over C

Question: How does the Frobenius depend on the labeling , choice of spanning tree, etc.?

Answer: You can identify the Galois group G(Y/X) with a quotient Γ/H, Γ= the fundamental group of X, a group which can be viewed as generated by the edges left out of a spanning tree.

Properties of Artin L-Functions

Copy from Lang, *Algebraic Number Theory*

1) L(u,1,Y/X) = ζ(u,X) = **Ihara zeta function** of X (our analog of the **Dedekind zeta** function, also **Selberg zeta)**

Proof by Defn.

2) $$\zeta(u,Y)=\prod_{\rho\in\widehat{G}} L(u,\rho,Y/X)^{d_\rho}$$

product over all irreducible reps of *G*, d_ρ=degree ρ.

Proof uses induced representations and decomposition

$$Ind_{\{e\}}^{G} 1=\sum_{\pi\in\hat{G}}^{\oplus} d_\pi \pi$$

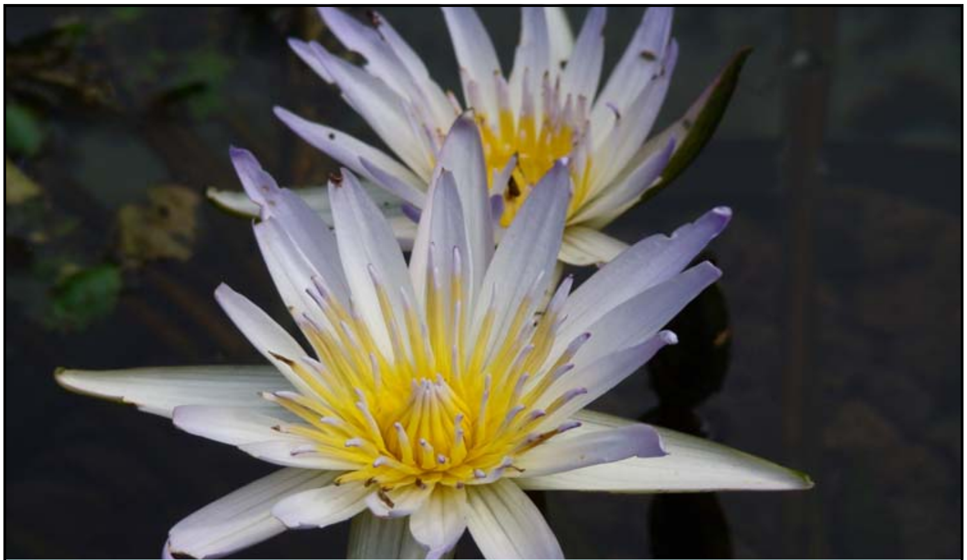
See A. T., *Fourier Analysis on Finite Groups and Applications.*

Det(I-uW$_1$) formula for Artin L-Functions

Set B=W$_1$ and call the Frobenius automorphism of an edge Frob(e). Define the blocks of the matrix 2|E|*d_ρ x 2|E|*d_ρ matrix B_ρ as follows, for each pair of oriented edges e,f in X :

$$\left(B_\rho\right)_{ef}=\left(b_{ef}\,\rho(Frob(e))\right)$$

$$L(u,\rho,Y/X)^{-1}=\det(I-uB_\rho)$$



For the cube over K_4 we have 2 degree 1 representations of the Galois group. The only interesting matrix is that for the non-trivial representation: 12x12 matrix. It is too big to put on a Power Point talk or blackboard.

Ihara Theorem for L-Functions

$$L(u,\rho,Y/X)^{-1}$$
$$=(1-u^2)^{(r-1)d}\det(I'-A'_\rho u+Q'u^2)$$

r=rank fundamental group of X = |E|-|V|+1

ρ= representation of G = Gal(Y/X), d = d_ρ = degree ρ

Definitions. nd×nd matrices A', Q', I', n=|X|,

nxn matrix A(g), g ∈ Gal(Y/X), entry for a,b vertices in X

$(A(g))_{a,b}$ = #{ edges in Y from (a,e) to (b,g) },

e=identity ∈ G.

$$A'_\rho=\sum_{g\in G}A(g)\otimes\rho(g)$$

Q = diagonal matrix, jth diagonal entry = q_j = (degree of jth vertex in X)-1,

$Q' = Q\otimes I_d$, $I' = I_{nd}$ = identity matrix.

$$B \otimes C = \begin{pmatrix} b_{11}C & \cdots & b_{1p}C \\ \vdots & \ddots & \vdots \\ b_{p1}C & \cdots & b_{pp}C \end{pmatrix}.$$

B is pxp and C is qxq
B⊗C is pqxpq

EXAMPLE

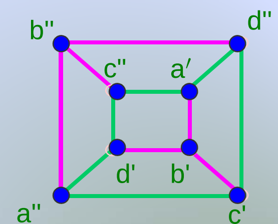
Y=cube, X=tetrahedron: $G = \{e,g\}$
representations of G are 1 and ρ: ρ(e) = 1, ρ(g) = -1
$A(e)_{u,v}$ = #{ length 1 paths u′ to v′ in Y}
$A(g)_{u,v}$ = #{ length 1 paths u′ to v″ in Y}

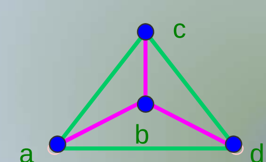
(u,e)=u′,
(u,g)=u″

A'_1 = A = adjacency matrix of X =A(e)+A(g)

$$A(e) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad A(g) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$A'_\rho = A(e) - A(g) = \begin{pmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & 1 \\ -1 & 1 & 0 & -1 \\ -1 & 1 & -1 & 0 \end{pmatrix}$$



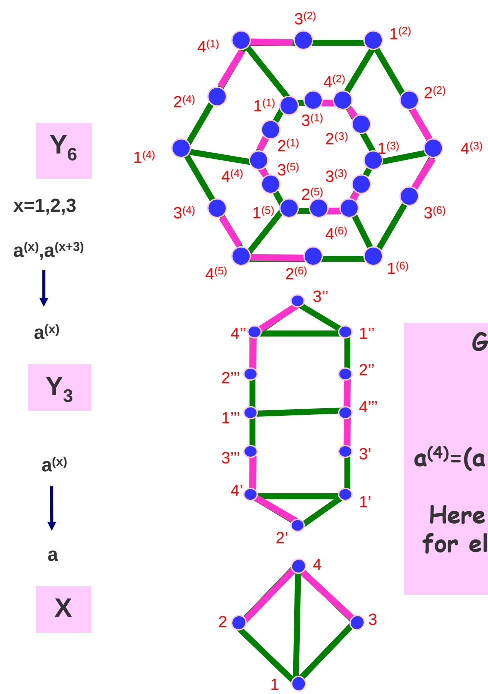


Zeta and L-Functions of Cube & Tetrahedron

$X = K_4$ and Y=cube

- $\zeta(u,X)^{-1} = (1-u^2)^2(1-u)(1-2u)\ (1+u+2u^2)^3$
- $L(u,\rho,Y/X)^{-1} = (1-u^2)\ (1+u)\ (1+2u)\ (1-u+2u^2)^3$
- $\zeta(u,Y)^{-1} = L(u,\rho,Y/X)^{-1}\ \zeta(u,X)^{-1}$

Get L function of $\zeta(u,X)$ by replacing u by -u for this example.



Example

Galois Cover of Non-Normal Cubic

$G=S_3$, $H=\{(1),(23)\}$ fixes Y_3.

$a^{(1)}=(a,(1))$, $a^{(2)}=(a,(13))$, $a^{(3)}=(a,(132)$, $a^{(4)}=(a,(23))$, $a^{(5)}=(a,(123))$, $a^{(6)}=(a,(12))$.

Here we use standard cycle notation for elements of the symmetric group.

Prime Splitting Completely

path in X (list vertices)   14312412431

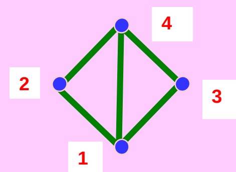
f=1, g=3   3 lifts to Y_3

1'4'3'''1'''2'''4''1''2''4'''3'1'

1''4''3''1''2''4'''1'''2'''4''3''1''

1'''4'''3'1'2'4'1'2'4'3'''1'''

Frobenius trivial $\Rightarrow$ density 1/6



This is an analog of the prime 31 for $\mathbb{Q}(2^{1/3})$ in Stark's article in From Number Theory to Physics, M. Waldschmidt et al (Eds.), Springer-Verlag, Berlin, 1992, pages 313-393.

Ihara Zeta Functions

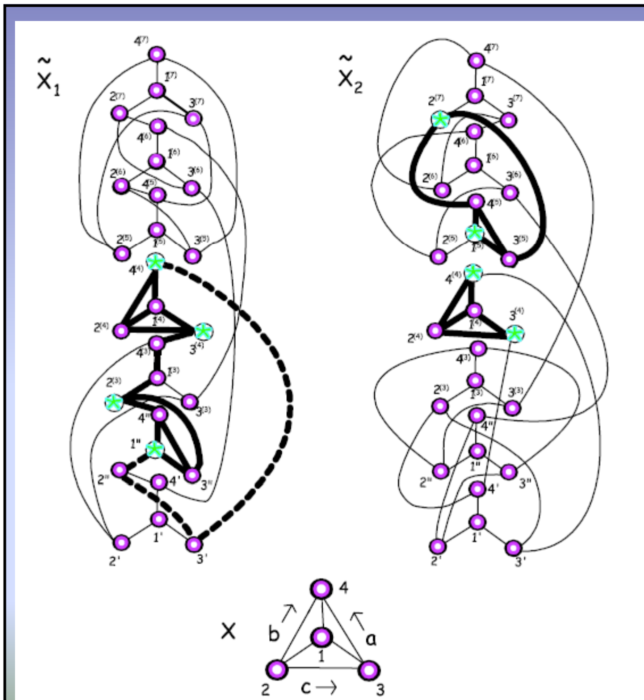
- $\zeta(u,X)^{-1} = (1-u^2)(1-u)(1+u^2)(1+u+2u^2)(1-u^2-2u^3)$
- $\zeta(u,Y_3)^{-1} = \zeta(u,X)^{-1} * (1-u^2)^2(1-u-u^3+2u^4)$
  $* (1+u+2u^2+u^3+2u^4)(1-u+2u^2-u^3+2u^4)(1+u+u^3+2u^4)$
- $\zeta(u,Y_6)^{-1} = \zeta(u,Y_3)^{-1} (1-u^2)^3 (1+u)(1+u^2)(1-u+2u^2)(1-u^2+2u^3)$
  $* (1-u-u^3+2u^4)(1-u+2u^2-u^3+2u^4)$
  $* (1+u+u^3+2u^4)(1+u+2u^2+u^3+2u^4)$

It follows that, as in number theory

$$\zeta(u,X)^2 \zeta(u,Y_6) = \zeta(u,Y_2) \zeta(u,Y_3)^2$$

Y_2 is an intermediate quadratic extension between Y_6 and X.

See Stark & Terras, *Adv. in Math.*, 154 (2000), Fig. 13, for more info.



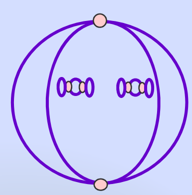
Application of Galois Theory of Graph Coverings.

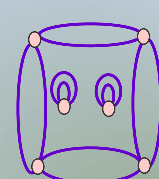
You can't hear the shape of a graph.

2 connected regular graphs (without loops & multiple edges) which are isospectral but not isomorphic

⌘ See A.T. & Stark in *Adv. in Math.*, Vol. 154 (2000) for the details. The method goes back to algebraic number theorists who found number fields K_i which are non isomorphic but have the same Dedekind zeta. See Perlis, *J. Number Theory*, 9 (1977).

⌘ Robert Perlis and Aubi Mellein have used the same methods to find many examples of isospectral non isomorphic graphs with multiple edges and components. 2 such are on the right.


Audrey


Harold

There are nice constructions of isospectral non-isomorphic graphs in paper of Lubotzky, Samuels and Vishne

Homework Problems

What are ramified coverings of graphs? Do the zetas^{-1} divide?

Is there a graph analog of regulator, Stark Conjectures, class field theory for abelian graph coverings? Or more simply a quadratic reciprocity law, fundamental units? The ideal class group is the Jacobian of a graph and has order = number of spanning trees (paper of Roland Bacher, Pierre de la Harpe and Tatiana Nagnibeda). There is an analog of Brauer-Siegel theory (see H.S. and A.T. , Part III).

See M. Baker and S. Norine, Harmonic morphisms and hyperelliptic graphs, preprint.

Beth Malmskog & Michelle Manes, Almost divisibility I the Ihara zeta functions of certain ramified covers of q+1-regular graphs, preprint.