

On the orientable genus of a zero divisor graph

Nathan Bloomfield

Dr. Cameron Wickham, advisor

Recall that a ring is a set R such that we can ‘add’ ‘subtract’ and ‘multiply’ within R . We will focus only on rings which are finite and commutative, and which have a nonzero multiplicative identity.

Examples: \mathbb{Z}_n , $\mathbb{Z}_2[x]/(x^2)$, $\mathbb{Z}_p \times \mathbb{Z}_q$

Much of ring theory is motivated by the abstraction of the properties of \mathbb{Z} .

Important Theorem: Every finite commutative ring is isomorphic to a direct product of finite commutative *local* rings, unique up to a permutation of the factors.

This result allows us to study (finite commutative) rings in two chunks: local and nonlocal.

A *subring* is a subset of a ring that satisfies the ring axioms. There is a special type of subring called an *ideal*; this has the additional property that the product of any ring element with any ideal element is in the ideal.

For example, $15\mathbb{Z}$ is an ideal of \mathbb{Z} .

An ideal is *maximal* if it is a largest nontrivial ideal. In general, a ring can have many maximal ideals.

Counterexample: $15\mathbb{Z}$ is not a maximal ideal of \mathbb{Z} because $15\mathbb{Z} \subset 3\mathbb{Z}$.

A ring is local if it has one and only one maximal ideal.

Example 1: The finite field \mathbb{F}_{p^α} is local; it has only the zero ideal.

Example 2: \mathbb{Z}_{12} is not local; $\{0, 2, 4, 6, 8, 10\}$ and $\{0, 3, 6, 9\}$ are both maximal ideals.

We can define a product on ideals as follows:

$$IJ = \{\sum ij : i \in I, j \in J\}$$

The product of two ideals is an ideal.

We can take powers of an ideal with recursive multiplication.

Important Theorem: If R is a local ring with maximal ideal M , then there is an integer n (called the *index of nilpotency*) such that $M^n \neq 0$ and $M^{n+1} = 0$.

Ring elements may not have multiplicative inverses. This means we may have elements $r \neq 0$ and $s \neq 0$ such that $rs = 0$. In a sense, r and s divide zero- so we call them
(nonzero) *zero-divisors*.

In a local ring, the zero divisors are precisely the nonzero elements of the maximal ideal.

Recall that a *graph* consists of a set of vertices and a set of edges among them.

Graphs can be imbedded in (drawn on) surfaces.

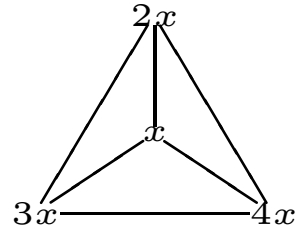
The *crossing number* of a graph G with respect to a surface S is the smallest n such that G can be imbedded in S with n edge crossings.

The *orientable genus* of a graph G is the smallest k such that the crossing number of G with respect to the k -handled sphere is 0.

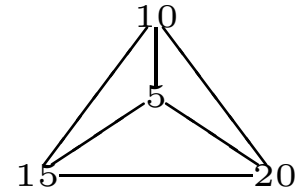
We can define the *zero-divisor graph* of a ring R (denoted $\Gamma(R)$) as follows:

- Vertices are the nonzero zero-divisors of R
- Two vertices are adjacent if their product is zero

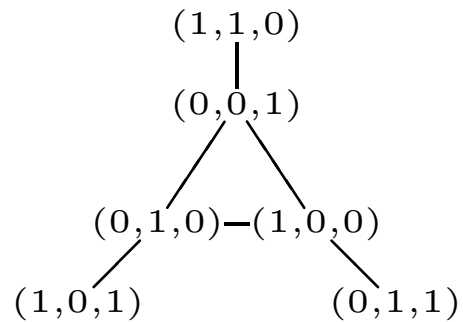
The zero-divisor graph preserves information about the annihilator structure of a ring.



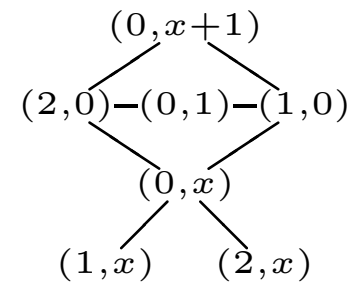
$$\Gamma(\mathbb{Z}_5[x]/(x^2))$$



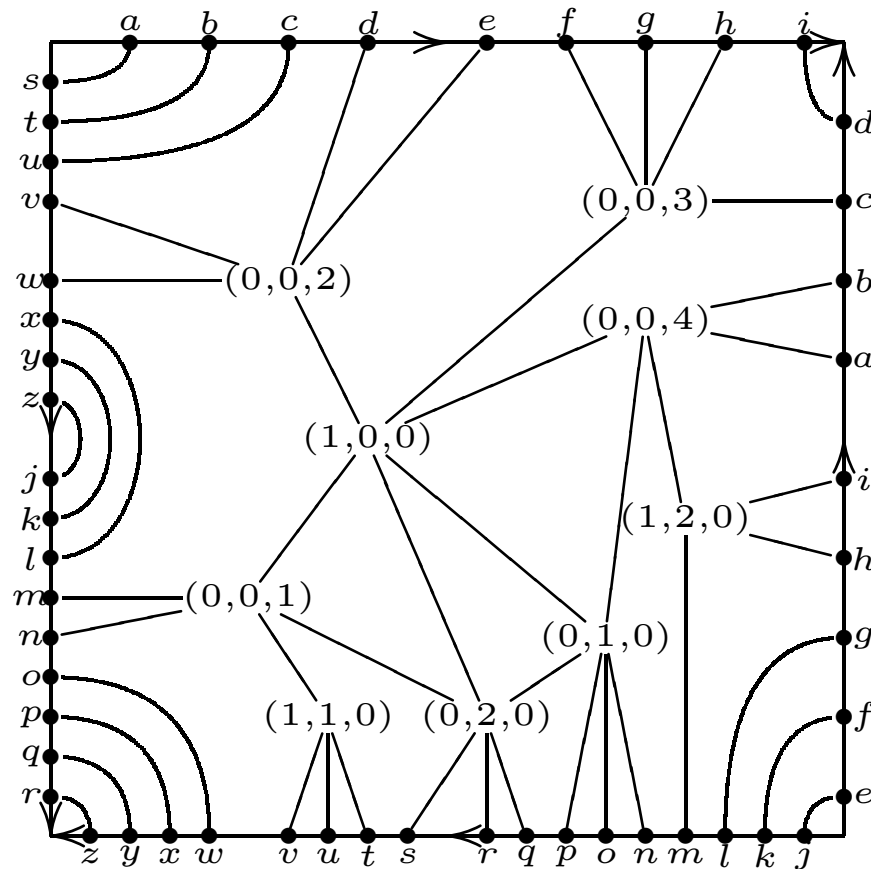
$$\Gamma(\mathbb{Z}_{25})$$



$$\Gamma(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$$



$$\Gamma(\mathbb{Z}_3 \times \mathbb{Z}_2[x]/(x^2))$$



$$\Gamma(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5)$$

We can determine two lower bounds for the genus of a zero divisor graph: one for local rings and one for nonlocal rings. Both work by constructing a complete or complete bipartite subgraph of $\Gamma(R)$.

If R is local with $|R| = p^k$ and index of nilpotency n , then

$$\gamma(\Gamma(R)) \geq \left\lceil \frac{1}{12} \left(p^{\lfloor \frac{n+1}{2} \rfloor} - 4 \right) \left(p^{\lfloor \frac{n+1}{2} \rfloor} - 5 \right) \right\rceil.$$

If R is not local with m local factors, then

$$\gamma(\Gamma(R)) \geq \left\lceil \frac{1}{4} \left(2^{\lfloor m/2 \rfloor} - 3 \right) \left(2^{\lceil m/2 \rceil} - 3 \right) \right\rceil.$$

To find all the finite commutative rings of genus g (in my case $g = 2$), we can use these bounds to eliminate all but a finite number of rings from consideration. Then the enumeration reduces to several pages of very boring case analysis.

However, along the way I encountered something not so boring...

We saw that $\Gamma(\mathbb{Z}_5[x]/(x^2))$ and $\Gamma(\mathbb{Z}_{25})$ are different rings with the same zero divisor graph – they have the same annihilator structure. This example motivates the following definition:

Two rings R and S are *isonihilate*, denoted $R \approx S$, if there is a bijection $\Phi : R \rightarrow S$ such that, for $r_1, r_2 \in R$, we have $r_1 r_2 = 0$ iff $\Phi(r_1)\Phi(r_2) = 0$.

\cong is an equivalence relation. Note that $R \cong S$ implies $\Gamma(R) \cong \Gamma(S)$, but not vice versa. Also, it's not hard to show that if $R_1 \cong R_2$ and $S_1 \cong S_2$, then

$$R_1 \times S_1 \cong R_2 \times S_2.$$

Now we can explain the anomaly from before.

Elements of $\mathbb{Z}_p[x]/(x^k)$ are polynomials in x with coefficients from \mathbb{Z}_p and degree less than k :

$$\pi(x) = \sum_{i=0}^{k-1} \alpha_i x^i, \alpha_i \in \mathbb{Z}_p.$$

Elements of \mathbb{Z}_p^k are p -adic numbers with less than k digits:

$$q = \sum_{i=0}^{k-1} \alpha_i p^i, \alpha_i \in \mathbb{Z}_p.$$

The function $\Phi(\pi(x)) = \pi(p)$ is bijective and preserves zero products. Hence, $\mathbb{Z}_p[x]/(x^k) \cong \mathbb{Z}_{p^k}$.

In fact, lots of rings are isonihilate to other rings.

Classifying rings according to their genus is, in the absence of a graph imbedding algorithm other than trial and error, Very Hard. By exploiting isonihilations, we can considerably reduce the amount of work necessary.

There is a lot of uncharted territory in the land of finite commutative rings. It is hoped that the study of zero divisor graphs can help illuminate the metastructure among rings.

From here, there are several open problems:

- What rings are orientable genus 3, 4, ... ?
- Are the local rings of order p^k partially ordered by the subgraph relation? Are the isonihilation classes totally ordered?
- Which zero divisor graphs are Hamiltonian?
- What about the zero divisor digraph of a noncommutative ring?