Local Rings of Order p^6

Charlie Scherer

October 24, 2008

Ideals

All rings are assumed to be commutative and to have identity. R always denotes such a ring.

Definition

Recall that an ideal is an additive subgroup, I, such that $rI \subset I$ for all $r \in R$. A maximal ideal is a proper ideal, M, which is not contained in any other proper ideal.

Ideals

All rings are assumed to be commutative and to have identity. R always denotes such a ring.

Definition

Recall that an ideal is an additive subgroup, I, such that $rI \subset I$ for all $r \in R$. A maximal ideal is a proper ideal, M, which is not contained in any other proper ideal.

(Warning: Axiom of Choice) All rings have a maximal ideal. Some rings have more than one.

Ideals

All rings are assumed to be commutative and to have identity. R always denotes such a ring.

Definition

Recall that an ideal is an additive subgroup, I*, such that* $rI \subset I$ *for all* $r \in R$*. A maximal ideal is a proper ideal,* M*, which is not contained in any other proper ideal.*

(Warning: Axiom of Choice) All rings have a maximal ideal. Some rings have more than one.
Examples:

1. $\mathbb{R}[X]$, (X)

Ideals

All rings are assumed to be commutative and to have identity. R always denotes such a ring.

Definition

Recall that an ideal is an additive subgroup, I, such that $rI \subset I$ for all $r \in R$. A maximal ideal is a proper ideal, M, which is not contained in any other proper ideal.

(Warning: Axiom of Choice) All rings have a maximal ideal. Some rings have more than one.
Examples:

1. $\mathbb{R}[X]$, (X)
2. $\mathbb{Z}$, (p) for any prime p

Ideals

All rings are assumed to be commutative and to have identity. R always denotes such a ring.

Definition

Recall that an ideal is an additive subgroup, I, such that $rI \subset I$ for all $r \in R$. A maximal ideal is a proper ideal, M, which is not contained in any other proper ideal.

(Warning: Axiom of Choice) All rings have a maximal ideal. Some rings have more than one.
Examples:

1. $\mathbb{R}[X]$, (X)
2. $\mathbb{Z}$, (p) for any prime p
3. $\mathbb{Q}$, $\{0\}$

Ideals, cont.

Definition

The product of two ideals, I and J, is

$$\left\{ \sum a_i b_i \mid a_i \in I \text{ and } b_i \in J \text{ for } i = 1, ..., n \text{ for some } n \in \mathbb{Z}^+ \right\}$$

Ideals, cont.

Definition

The product of two ideals, I and J, is

$$\left\{ \sum a_i b_i \mid a_i \in I \text{ and } b_i \in J \text{ for } i = 1, ..., n \text{ for some } n \in \mathbb{Z}^+ \right\}$$

Examples:

1. In $\mathbb{R}[X]$, $(X)(X+1) = (X^2 + X)$.

Ideals, cont.

Definition

The product of two ideals, I and J, is

$$\left\{\sum a_i b_i \mid a_i \in I \text{ and } b_i \in J \text{ for } i = 1, \ldots, n \text{ for some } n \in \mathbb{Z}^+\right\}$$

Examples:

1. In $\mathbb{R}[X]$, $(X)(X+1) = (X^2 + X)$.
2. In $\mathbb{Q}[X, Y, Z]$ $(X, Y)(Y, Z) = (XY, XZ, Y^2, YZ)$.

Ideals, cont.

Definition

The product of two ideals, I and J, is

$$\left\{ \sum a_i b_i \mid a_i \in I \text{ and } b_i \in J \text{ for } i = 1, \ldots, n \text{ for some } n \in \mathbb{Z}^+ \right\}$$

Examples:

1. In $\mathbb{R}[X]$, $(X)(X+1) = (X^2 + X)$.
2. In $\mathbb{Q}[X, Y, Z]$ $(X, Y)(Y, Z) = (XY, XZ, Y^2, YZ)$.
3. In $\mathbb{Z}_6$, $(2)(2) = (2)$.

Ideals, cont.

Definition

The product of two ideals, I and J, is

$$\left\{ \sum a_i b_i \mid a_i \in I \text{ and } b_i \in J \text{ for } i = 1, \ldots, n \text{ for some } n \in \mathbb{Z}^+ \right\}$$

Examples:

1. In $\mathbb{R}[X]$, $(X)(X+1) = (X^2 + X)$.
2. In $\mathbb{Q}[X, Y, Z]$ $(X, Y)(Y, Z) = (XY, XZ, Y^2, YZ)$.
3. In $\mathbb{Z}_6$, $(2)(2) = (2)$.

$IJ \subset I \cap J$, in particular, $I^2 \subset I$ containment may or may not be strict.

Local Rings

Definition

A local ring denoted, (R, M)*, is a ring with a unique maximal ideal,* M*.*

Local Rings

Definition

A local ring denoted, (R, M), is a ring with a unique maximal ideal, M.

(Warning: Axiom of Choice) Every non-unit is contained in some maximal ideal.

Local Rings, cont.

Examples of local rings:

1. $\mathbb{R}[X]$ is not a local ring.

Local Rings, cont.

Examples of local rings:

1. $\mathbb{R}[X]$ is not a local ring.
2. $\mathbb{Z}$ is not a local ring.

Local Rings, cont.

Examples of local rings:

1. $\mathbb{R}[X]$ is not a local ring.
2. $\mathbb{Z}$ is not a local ring.
3. $\mathbb{Q}$ is a field. All fields are local rings.

Local Rings, cont.

Examples of local rings:

1. $\mathbb{R}[X]$ is not a local ring.
2. $\mathbb{Z}$ is not a local ring.
3. $\mathbb{Q}$ is a field. All fields are local rings.
4. $R_G = \frac{\mathbb{Z}_p[X_1,\ldots,X_n]}{(X_i X_j)}$ is a local ring of order p^{n+1} whose maximal ideal is $(X_1, X_2, \ldots, X_n)$.

Local Rings, cont.

Examples of local rings:

1. $\mathbb{R}[X]$ is not a local ring.
2. $\mathbb{Z}$ is not a local ring.
3. $\mathbb{Q}$ is a field. All fields are local rings.
4. $R_G = \frac{\mathbb{Z}_p[X_1,\ldots,X_n]}{(X_i X_j)}$ is a local ring of order p^{n+1} whose maximal ideal is $(X_1, X_2, \ldots, X_n)$.
5. $R_{g^2} = \frac{\mathbb{Z}_p[X,Y]}{(X^2, f(Y))}$ is a local ring where $f(Y)$ is a polynomial of degree n, irreducible modulo p. Its order is p^{2n} and it's maximal ideal is (X).

Galois Rings

Definition

Let p be a prime and k be a positive integer and suppose that $f(X)$ is a polynomial of degree r irreducible modulo p. Then we call $\frac{\mathbb{Z}_{p^k}[X]}{(f(X))}$ a Galois ring and denote it $G(p^k, r)$.

Galois Rings

Definition

Let p be a prime and k be a positive integer and suppose that $f(X)$ is a polynomial of degree r irreducible modulo p. Then we call $\frac{\mathbb{Z}_{p^k}[X]}{(f(X))}$ a Galois ring and denote it $G(p^k, r)$.

Examples:

1. $G(p^k, 1) = \mathbb{Z}_{p^k}$.

Galois Rings

Definition

Let p be a prime and k be a positive integer and suppose that $f(X)$ is a polynomial of degree r irreducible modulo p. Then we call $\frac{\mathbb{Z}_{p^k}[X]}{(f(X))}$ a Galois ring and denote it $G(p^k, r)$.

Examples:

1. $G(p^k, 1) = \mathbb{Z}_{p^k}$.
2. $G(p, r) = \mathbb{F}_{p^r}$.

Facts About Local Rings

Let (R, M) be a finite local ring.

Lemma (Nakayama)

If I is an ideal of R then $IM = I$ iff $I = 0$.

Facts About Local Rings

Let (R, M) be a finite local ring.

Lemma (Nakayama)

If I is an ideal of R then $IM = I$ iff $I = 0$.

This means we can form the sequence of nested ideals, $M \supsetneq M^2 \supsetneq \dots \supsetneq M^{t-1} \supsetneq M^t = 0$.

Facts About Local Rings

Let (R, M) be a finite local ring.

Lemma (Nakayama)

If I is an ideal of R then $IM = I$ iff $I = 0$.

This means we can form the sequence of nested ideals,
$M \supsetneq M^2 \supsetneq ... \supsetneq M^{t-1} \supsetneq M^t = 0$.

Lemma

M^k/M^{k+1} is a vector space over R/M for all positive integers k.

Facts About Local Rings

Let (R, M) be a finite local ring.

Lemma (Nakayama)

If I is an ideal of R then $IM = I$ iff $I = 0$.

This means we can form the sequence of nested ideals,
$M \supsetneq M^2 \supsetneq \ldots \supsetneq M^{t-1} \supsetneq M^t = 0$.

Lemma

M^k/M^{k+1} is a vector space over R/M for all positive integers k.

Corollary

Any two minimal generating sets for M^k are the same size, $dim_{R/M} M^k/M^{k+1}$.

Facts About Local Rings

Let (R, M) be a finite local ring.

Lemma (Nakayama)

If I is an ideal of R then $IM = I$ iff $I = 0$.

This means we can form the sequence of nested ideals,
$M \supsetneq M^2 \supsetneq \dots \supsetneq M^{t-1} \supsetneq M^t = 0$.

Lemma

M^k/M^{k+1} is a vector space over R/M for all positive integers k.

Corollary

Any two minimal generating sets for M^k are the same size, $dim_{R/M} M^k/M^{k+1}$.

Corollary

$|R| = |R/M|^q$ for some prime p and positive integer q.

Facts About Local Rings

Let (R, M) be a finite local ring.

Lemma (Nakayama)

If I is an ideal of R then $IM = I$ iff $I = 0$.

This means we can form the sequence of nested ideals, $M \supsetneq M^2 \supsetneq \ldots \supsetneq M^{t-1} \supsetneq M^t = 0$.

Lemma

M^k/M^{k+1} is a vector space over R/M for all positive integers k.

Corollary

Any two minimal generating sets for M^k are the same size, $dim_{R/M} M^k/M^{k+1}$.

Corollary

$|R| = |R/M|^q$ for some prime p and positive integer q.

Corollary

$|R| = p^n$ for some prime p and positive integer n.

The Structure Theorem

Theorem (General Structure Theorem)

Let (R, M) be a local ring of characteristic p^k. Let $r = [R/M : \mathbb{Z}_p]$ and suppose M is minimally generated by $x_1, x_2, ..., x_n$. Then:

1. *$G(p^k, r) \leq R$ and $G(p^k, r)$ is the largest Galois ring in R.*
2. *$G(p^k, r)[X_1, X_2, ..., X_n] \twoheadrightarrow R$ in such a way that $X_i \mapsto x_i$ for $i = 1, 2, ..., n$*

The Structure Theorem, cont.

Example:
Suppose we want to know which rings of order p^5 have characteristic p and have $M^2 = 0$...

The Structure Theorem, cont.

Example:
Suppose we want to know which rings of order p^5 have characteristic p and have $M^2 = 0$...

1. We know $|R| = |R/M|^q$ therefore $q = 5$, ($q = 1 \iff R$ is a field).

The Structure Theorem, cont.

Example:
Suppose we want to know which rings of order p^5 have characteristic p and have $M^2 = 0$...

1. We know $|R| = |R/M|^q$ therefore $q = 5$, ($q = 1 \iff R$ is a field).
2. Take $q = 5$ and get $|M/M^2| = |M| = p^4$ since $M^{1+k}/M^{2+k} = 0$.

The Structure Theorem, cont.

Example:
Suppose we want to know which rings of order p^5 have characteristic p and have $M^2 = 0$...

1. We know $|R| = |R/M|^q$ therefore $q = 5$, ($q = 1 \iff R$ is a field).
2. Take $q = 5$ and get $|M/M^2| = |M| = p^4$ since $M^{1+k}/M^{2+k} = 0$.
3. Thus $G(p,1)[X_1, X_2, X_3, X_4] = \mathbb{Z}_p[X_1, X_2, X_3, X_4] \twoheadrightarrow R$.

The Structure Theorem, cont.

Example:
Suppose we want to know which rings of order p^5 have characteristic p and have $M^2 = 0$...

1. We know $|R| = |R/M|^q$ therefore $q = 5$, ($q = 1 \iff R$ is a field).
2. Take $q = 5$ and get $|M/M^2| = |M| = p^4$ since $M^{1+k}/M^{2+k} = 0$.
3. Thus $G(p,1)[X_1, X_2, X_3, X_4] = \mathbb{Z}_p[X_1, X_2, X_3, X_4] \twoheadrightarrow R$.
4. Since $M^2 = 0$, $\frac{\mathbb{Z}_p[X_1,X_2,X_3,X_4]}{(X_iX_j)} \twoheadrightarrow R$

The Structure Theorem, cont.

Example:
Suppose we want to know which rings of order p^5 have characteristic p and have $M^2 = 0$...

1. We know $|R| = |R/M|^q$ therefore $q = 5$, ($q = 1 \iff R$ is a field).
2. Take $q = 5$ and get $|M/M^2| = |M| = p^4$ since $M^{1+k}/M^{2+k} = 0$.
3. Thus $G(p,1)[X_1, X_2, X_3, X_4] = \mathbb{Z}_p[X_1, X_2, X_3, X_4] \twoheadrightarrow R$.
4. Since $M^2 = 0$, $\frac{\mathbb{Z}_p[X_1,X_2,X_3,X_4]}{(X_iX_j)} \twoheadrightarrow R$
5. Conclude these two are actually isomorphic.

Abridged Catalogue

$\lvert M\rvert$	$\lvert M^2\rvert$	$\lvert M^3\rvert$	$\lvert M^4\rvert$	$\lvert M^5\rvert$	$char R$	R
p^3	0	0	0	0	p	$\frac{G(p,3)[X]}{(X^2)}$
p^3	0	0	0	0	p^2	$G(p^2,3)$
p^4	0	0	0	0	p	$\frac{G(p,2)[X,Y]}{(X^2,XY,Y^2)}$
p^4	0	0	0	0	p^2	$\frac{G(p^2,2)[X,Y]}{(X^2,pX,Y-p)} \simeq \frac{G(p^2,2)[X]}{(X^2,pX)}$
p^4	p^2	0	0	0	p	$\frac{G(p,2)[X]}{(X^3)}$
p^4	p^2	0	0	0	p^2	$\frac{G(p^2,2)[X]}{(X^3,X^2-p)}$ $\frac{G(p^2,2)[X]}{(X^3,X^2-np)}$ $n \notin (U(\mathbb{Z}_{p^2}))^2$
p^4	p^2	0	0	0	p^3	$G(p^2,3)$
p^5	0	0	0	0	p	$\frac{G(p,1)[X_1,X_2,X_3,X_4,X_5]}{(X_iX_j)_{i,j=1,2,3,4,5}}$
p^5	0	0	0	0	p^2	$\frac{G(p^2,1)[X_1,X_2,X_3,X_4,X_5]}{(X_iX_j,X_5-p)_{i,j=1,2,3,4,5}}$
p^5	p^3	p^2	p	0	p	$\frac{G(p,1)[X_1,X_2]}{(X_1X_2,X_2^2,X_1^5)}$
p^5	p^4	p^3	p^2	p	p	$\frac{G(p,1)[X]}{(X^6)}$

A Specific Case

What about when $|M| = p^5$, $|M^2| = p$ and $charR = p$?

1. Identify all rings of this type with a matrix with entries from $\mathbb{Z}_p$.

A Specific Case

What about when $|M| = p^5$, $|M^2| = p$ and $charR = p$?

1. Identify all rings of this type with a matrix with entries from $\mathbb{Z}_p$.
2. Identify isomorphisms of these rings with matrices of the same type.

A Specific Case

What about when $|M| = p^5$, $|M^2| = p$ and $charR = p$?

1. Identify all rings of this type with a matrix with entries from $\mathbb{Z}_p$.
2. Identify isomorphisms of these rings with matrices of the same type.
3. A question of ring isomorphisms becomes a question of linear algebra!

A Specific Case, Step 1

Given (R, M) of characteristic p such that $|R| = p^6$, $|M| = p^5$ and $|M^2| = p$, we know:

A Specific Case, Step 1

Given (R, M) of characteristic p such that $|R| = p^6$, $|M| = p^5$ and $|M^2| = p$, we know:

1. $M = (x_1, x_2, x_3, x_4)$

A Specific Case, Step 1

Given (R, M) of characteristic p such that $|R| = p^6$, $|M| = p^5$ and $|M^2| = p$, we know:

1. $M = (x_1, x_2, x_3, x_4)$
2. $M^2 = (y)$

A Specific Case, Step 1

Given (R, M) of characteristic p such that $|R| = p^6$, $|M| = p^5$ and $|M^2| = p$, we know:

1. $M = (x_1, x_2, x_3, x_4)$
2. $M^2 = (y)$
3. Therefore $x_i x_j = n_{i,j} y$ for some $n_{i,j} \in \mathbb{Z}_p$.

A Specific Case, Step 1

Given (R, M) of characteristic p such that $|R| = p^6$, $|M| = p^5$ and $|M^2| = p$, we know:

1. $M = (x_1, x_2, x_3, x_4)$
2. $M^2 = (y)$
3. Therefore $x_i x_j = n_{i,j} y$ for some $n_{i,j} \in \mathbb{Z}_p$.

So define $N = (n_{i,j})$ and we get a correspondence between rings and matrices over $\mathbb{Z}_p$.

Let $\bar{x} = (x_1\, x_2\, x_3\, x_4)$ and note that $\bar{x}^\top \bar{x} = yN$.

A Specific Case, Step 2

Given an isomorphism $(R, M) \xrightarrow{\phi} (R', M')$, we know that $\phi[M] = M'$ so that:

A Specific Case, Step 2

Given an isomorphism $(R, M) \xrightarrow{\phi} (R', M')$, we know that $\phi[M] = M'$ so that:

1. $x_i \mapsto \sum p_{i,j} x'_j + r_i y'$.

A Specific Case, Step 2

Given an isomorphism $(R, M) \xrightarrow{\phi} (R', M')$, we know that $\phi[M] = M'$ so that:

1. $x_i \mapsto \sum p_{i,j} x'_j + r_i y'$.
2. We can assume $r_i = 0$ for all $i = 1, 2, 3, 4$.

A Specific Case, Step 2

Given an isomorphism $(R, M) \xrightarrow{\phi} (R', M')$, we know that $\phi[M] = M'$ so that:

1. $x_i \mapsto \sum p_{i,j} x'_j + r_i y'$.
2. We can assume $r_i = 0$ for all $i = 1, 2, 3, 4$.
3. $y \mapsto q y'$ for non-zero $q \in \mathbb{Z}_p$.

A Specific Case, Step 2

Given an isomorphism $(R, M) \xrightarrow{\phi} (R', M')$, we know that $\phi[M] = M'$ so that:

1. $x_i \mapsto \sum p_{i,j} x'_j + r_i y'$.
2. We can assume $r_i = 0$ for all $i = 1, 2, 3, 4$.
3. $y \mapsto q y'$ for non-zero $q \in \mathbb{Z}_p$.

Note that $P(x_1\, x_2\, x_3\, x_4)^\top = (\phi(x_1)\, \phi(x_2)\, \phi(x_3)\, \phi(x_4))^\top$ so that $P\bar{x}^\top \bar{x} P^\top = q y' N'$.

A Specific Case, Step 3

Thus we have that $(R, M) \cong (R', M')$ iff there exists some P and q so that:
$P^\top NP = qN'$.

A Specific Case, Step 3

Thus we have that $(R, M) \cong (R', M')$ iff there exists some P and q so that:
$P^\top NP = qN'$.
Luckily this forms an equivalence relation on the $n \times n$ matrices over $\mathbb{Z}_p$, called projective congruence. So the question becomes:

A Specific Case, Step 3

Thus we have that $(R, M) \cong (R', M')$ iff there exists some P and q so that:
$P^\top NP = qN'$.
Luckily this forms an equivalence relation on the $n \times n$ matrices over $\mathbb{Z}_p$, called projective congruence. So the question becomes: What is a representative set for the equivalence classes?

A Specific Case, cont.

Lemma

Suppose $p \neq 2$ and let f be a non-square modulo $\mathbb{F}_{p^k}$. Then any symmetric $n \times n$ matrix, N, over $\mathbb{F}_p^q$ is projectively congruent to a matrix of the form:

$$\begin{bmatrix} \mathbf{I}_{r-1} & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

where r is the rank of N and $a = 1$ or $a = f$.

A Specific Case, cont.

Lemma

Suppose $p \neq 2$ and let f be a non-square modulo $\mathbb{F}_{p^k}$. Then any symmetric $n \times n$ matrix, N, over $\mathbb{F}_p^q$ is projectively congruent to a matrix of the form:

$$\begin{bmatrix} \mathbf{I}_{r-1} & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

where r is the rank of N and $a = 1$ or $a = f$.

This lemma tells us how to pick representatives of each isomorphism class of the types of rings we're interested.

Looking Towards the Future

1. Finish classifying local rings of order p^6.
2. Generalize this technique to classify local rings such that $M^3 = 0$.