Clean Rings

Oscar Vega

Fresno State. November 23^{rd}, 2010.

Rings.

Definition

A ring R is a nonempty set endowed with two (closed) binary operations, $+$ and $\cdot$, such that:

(i) $(R, +)$ is an Abelian group,

(ii) the associative law for $\cdot$ holds. That is,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

for all $a, b, c \in R$, and

(iii) the distributive laws hold. That is,

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \textit{and} \qquad (a + b) \cdot c = a \cdot c + b \cdot c$$

for all $a, b, c \in R$.

Rings and Things.

- If a ring R contains an element x such that

$$x \cdot a = a \cdot x = a$$

  for all $a \in R$, then x is called 'one' and R is said to be a ring with 1.

- Let R be a ring. If

$$a \cdot b = b \cdot a$$

  for all $a, b \in R$ then R is said to be a commutative ring.

Example

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$, for all $n \in \mathbb{Z}_+$, are commutative rings with one.
- $M_2(\mathbb{R})$ is not commutative but it has a one.
- $2\mathbb{Z}$ is a commutative ring without one.

Idempotents Я us.

Let R be a ring,

- $e \in R$ is an idempotent if $e^2 = e$.
- $u \in R$ is called an involution if $u^2 = 1$.

Exercise

Let R be a ring with 1,

1. *if e is an idempotent, then $u = 1 - 2e$ is an involution.*
2. *If 2 is invertible in R (with respect to $\cdot$) and u is an involution, then $2^{-1}(1 - u)$ is an idempotent.*
3. *If 2 is invertible in R, the two processes above are inverses of each other.*
4. *If R is finite and 2 is invertible in R, then the cardinality of the set of idempotents in R is equal to the cardinality of the set of involutions in R.*

Clean, Shaven.

Definition

Let R be a ring with one.

(i) R is clean if every $r \in R$ can be written as $r = e + u$, where e is an idempotent and u is invertible.

(ii) If R is clean then a set of idempotents $E \subset R$ such that every element in R can be written as $e + u$, where $e \in E$ and u is invertible, is called a clean set of idempotents.

(iii) The least cardinality among all clean sets of idempotents in a clean ring R is denoted $Opt(R)$.

Question

How to find $Opt(R)$?

The Usual Suspects.

- If F is a field, then F is clean and $Opt(F) = 2$.
- Since every element x in a local ring is such that either x or $1 - x$ is a unit, then every local ring R is clean and $Opt(R) = 2$.
- $\mathbb{Z}$ is not clean.
- Let p be a prime and $a \in \mathbb{Z}$. Then, $\mathbb{Z}_{p^a}$ is clean, and $Opt(\mathbb{Z}_{p^a}) = 2$.
- Matrices? Polynomials?

Direct Products.

- Let R_i be a clean ring for all $i \in I$. Then $R = \prod_{i \in I} R_i$ is also clean, and every clean set of idempotents E of R contains $\prod_{i \in I} E_i$, where each E_i is a minimal set of idempotents of R_i. In particular, if $I = \{1, 2, \cdots, n\}$,
$$Opt(R) = \prod_{i=1}^{n} Opt(R_i)$$

- Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the prime factorization of $n \in \mathbb{Z}_+$. Then, $\mathbb{Z}_n$ is clean and $Opt(\mathbb{Z}_n) = 2^k$.

- It is known that an Artinian ring is a finite product of local rings.

- It is also known that if R is a commutative clean ring and the number of idempotents of R is finite, then R is a finite direct product of local rings.

Other Results.

Lemma (REU Kids)

Suppose R is a clean ring, E a clean set of idempotents, and f is any idempotent in R. If we write $1 - f = e + u$, where $e \in E$ and u is a unit, then $f = u^{-1}eu$. In particular, every idempotent in R must be conjugate to an element in E.

Corollary

Let R be a clean ring, then $Opt(R)$ is at least the cardinality of the set of central idempotents in R. In particular, if R is commutative, then there is a unique set of clean idempotents, which is the set of all idempotents.

Conjugation.

- If $r = e + u$, where e is an idempotent and u is a unit, then srs^{-1} is the sum of the idempotent ses^{-1} and the unit sus^{-1}.
- It follows that in order to study clean rings we just need to study the representatives of the orbits of the action of R^* on R by conjugation.
- Note that if $R = M_n(F)$, where F is a field, the study of the orbits in R under $R^* = GL_n(F)$ is what we call linear algebra.

Matrices: Clean & Claim.

Theorem

$M_n(F)$ is clean, and $Opt(M_n(F)) \leq 2^n$, for any field F.

Claim

$Opt(M_n(F)) = 2^n$, for F a field.

Remark

If the previous claim is correct then we would be able to find $Opt(R)$ for all finite semisimple rings.

- It is known that the claim is true for $M_n(F)$, $F = \mathbb{R}, \mathbb{C}$, $n \leq 4$.

Awful Bounds.

In order to prove the claim we have tried to find lower bounds for $Opt(M_n(F))$, but this seems not to be working very well. Firstly because we are considering only finite fields, and also because the bounds are not really optimal, as they tend to 1 when n goes to infinity.

Just for you to see how ugly these bounds are, here is one of the nicest we have found.

Let $\mathbb{F}_q$ be the field with q elements, then

$$Opt(M_n(\mathbb{F}_q)) \geq \frac{q^{n^2} - (q-2)^n}{q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1)\cdots(q-1) - (q-2)^n}$$

Any ideas? Please help!

Thank you.