Jacobson's Commutativity Theorem

Mike Daas

Universiteit Leiden

November 2nd, 2023

Prerequisites (1/3)

Groups

A *group* G is a set of things that we can *multiply*, write $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$, and we require that there are inverses; $g^{-1} \cdot g = 1 = g \cdot g^{-1}$.

Prerequisites (1/3)

Groups

A *group* G is a set of things that we can *multiply*, write $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$, and we require that there are inverses; $g^{-1} \cdot g = 1 = g \cdot g^{-1}$.

If $g \cdot h = h \cdot g$ for all $g, h \in G$, then G is *abelian* and write $\cdot = +$.

Prerequisites (1/3)

Groups

A *group* G is a set of things that we can *multiply*, write $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$, and we require that there are inverses; $g^{-1} \cdot g = 1 = g \cdot g^{-1}$.

If $g \cdot h = h \cdot g$ for all $g, h \in G$, then G is *abelian* and write $\cdot = +$.

Rings

A *ring* R is a set of things that we can *add* and *multiply*, write $g + h$ and $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$ and that everything works nicely (associative, distributative, etc...).

Important: We do *not* require that we have inverses for multiplication!

Prerequisites (1/3)

Groups

A *group* G is a set of things that we can *multiply*, write $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$, and we require that there are inverses; $g^{-1} \cdot g = 1 = g \cdot g^{-1}$.

If $g \cdot h = h \cdot g$ for all $g, h \in G$, then G is *abelian* and write $\cdot = +$.

Rings

A *ring* R is a set of things that we can *add* and *multiply*, write $g + h$ and $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$ and that everything works nicely (associative, distributative, etc...).

Important: We do *not* require that we have inverses for multiplication! If we *do* have inverses (except 0) and R is commutative, then we say that the ring is a *field*. **Example:** $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

Prerequisites (1/3)

Groups

A *group* G is a set of things that we can *multiply*, write $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$, and we require that there are inverses; $g^{-1} \cdot g = 1 = g \cdot g^{-1}$.

If $g \cdot h = h \cdot g$ for all $g, h \in G$, then G is *abelian* and write $\cdot = +$.

Rings

A *ring* R is a set of things that we can *add* and *multiply*, write $g + h$ and $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$ and that everything works nicely (associative, distributative, etc...).

Important: We do *not* require that we have inverses for multiplication! If we *do* have inverses (except 0) and R is commutative, then we say that the ring is a *field*. **Example:** $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

- $\mathbb{Z}/p\mathbb{Z}$ for p prime is a field; typically denoted $\mathbb{F}_p$.

Prerequisites (1/3)

Groups

A *group* G is a set of things that we can *multiply*, write $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$, and we require that there are inverses; $g^{-1} \cdot g = 1 = g \cdot g^{-1}$.

If $g \cdot h = h \cdot g$ for all $g, h \in G$, then G is *abelian* and write $\cdot = +$.

Rings

A *ring* R is a set of things that we can *add* and *multiply*, write $g + h$ and $g \cdot h$. We insist that there is a neutral element such that $1 \cdot g = g = g \cdot 1$ and that everything works nicely (associative, distributative, etc...).

Important: We do *not* require that we have inverses for multiplication! If we *do* have inverses (except 0) and R is commutative, then we say that the ring is a *field*. **Example:** $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

- $\mathbb{Z}/p\mathbb{Z}$ for p prime is a field; typically denoted $\mathbb{F}_p$.
- $\mathbb{Z}$ is a ring, but not a field. Similar for $\mathbb{Z}/4\mathbb{Z}$.

Prerequisites (2/3)

Proposition

For any prime p and positive integer k, there exists a unique finite field with p^k elements, denoted $\mathbb{F}_{p^k}$.

Prerequisites (2/3)

Proposition

For any prime p and positive integer k, there exists a unique finite field with p^k elements, denoted $\mathbb{F}_{p^k}$.

Another important example of rings:

$$R[X] = \{a_n X^n + \ldots + a_0 \mid a_i \in R\}.$$

Prerequisites (2/3)

Proposition

For any prime p and positive integer k, there exists a unique finite field with p^k elements, denoted $\mathbb{F}_{p^k}$.

Another important example of rings:

$$R[X] = \{a_n X^n + \ldots + a_0 \mid a_i \in R\}.$$

- If $x \cdot y = 0$ implies $x = 0$ or $y = 0$, then we say R is an *integral domain*. **Example**: $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain; $2 \cdot 3 = 0$.

Prerequisites (2/3)

Proposition

For any prime p and positive integer k, there exists a unique finite field with p^k elements, denoted $\mathbb{F}_{p^k}$.

Another important example of rings:

$$R[X] = \{a_n X^n + \ldots + a_0 \mid a_i \in R\}.$$

- If $x \cdot y = 0$ implies $x = 0$ or $y = 0$, then we say R is an *integral domain*. **Example**: $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain; $2 \cdot 3 = 0$.
- We say some $x \in R$ is *idempotent* if $x^2 = x$. **Examples**: $x \in \{0, 1\}$. More interestingly, $x = 3$ in $\mathbb{Z}/6\mathbb{Z}$.

Prerequisites (2/3)

Proposition

For any prime p and positive integer k, there exists a unique finite field with p^k elements, denoted $\mathbb{F}_{p^k}$.

Another important example of rings:

$$R[X] = \{a_n X^n + \ldots + a_0 \mid a_i \in R\}.$$

- If $x \cdot y = 0$ implies $x = 0$ or $y = 0$, then we say R is an *integral domain*. **Example**: $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain; $2 \cdot 3 = 0$.
- We say some $x \in R$ is *idempotent* if $x^2 = x$. **Examples**: $x \in \{0, 1\}$. More interestingly, $x = 3$ in $\mathbb{Z}/6\mathbb{Z}$.
- We say a ring R is *reduced* if $x^2 = 0 \implies x = 0$. **Examples**: all fields are reduced, but so is $\mathbb{Z}/6\mathbb{Z}$. However, $\mathbb{Z}/4\mathbb{Z}$ is not reduced.

Prerequisites (2/3)

Proposition

For any prime p and positive integer k, there exists a unique finite field with p^k elements, denoted $\mathbb{F}_{p^k}$.

Another important example of rings:

$$R[X] = \{a_n X^n + \ldots + a_0 \mid a_i \in R\}.$$

- If $x \cdot y = 0$ implies $x = 0$ or $y = 0$, then we say R is an *integral domain*. **Example**: $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain; $2 \cdot 3 = 0$.
- We say some $x \in R$ is *idempotent* if $x^2 = x$. **Examples**: $x \in \{0, 1\}$. More interestingly, $x = 3$ in $\mathbb{Z}/6\mathbb{Z}$.
- We say a ring R is *reduced* if $x^2 = 0 \implies x = 0$. **Examples**: all fields are reduced, but so is $\mathbb{Z}/6\mathbb{Z}$. However, $\mathbb{Z}/4\mathbb{Z}$ is not reduced.
- Multiplication in R need not be commutative. Define the *center* of R to be $Z(R) = \{x \in R \mid xy = yx \text{ for all } y \in R\}$. This is a subring. **Example**: if $R = \mathrm{Mat}_n(\mathbb{C})$, then $Z(R) = \{\lambda \cdot \mathrm{id}_n \mid \lambda \in \mathbb{C}\} \cong \mathbb{C}$.

Prerequisites (3/3)

We say some $x \in R$ is a *unit* if $xy = 1 = yx$ for some $y \in R$. Denote $R^\times = \{x \in R \mid x \text{ is a unit.}\}$. Then $R^\times$ is a group, and $1 \in R^\times$.

Prerequisites (3/3)

We say some $x \in R$ is a *unit* if $xy = 1 = yx$ for some $y \in R$. Denote $R^\times = \{x \in R \mid x \text{ is a unit.}\}$. Then $R^\times$ is a group, and $1 \in R^\times$.

Proposition

For any finite field $\mathbb{F}_{p^k}$, the group $\mathbb{F}_{p^k}^\times = \mathbb{F}_{p^k} \setminus \{0\}$ is *cyclic*, i.e. it is isomorphic to $\mathbb{Z}/(p^k - 1)\mathbb{Z}$. In fact, $x^{p^k} = x \iff x \in \mathbb{F}_{p^k} \subset \overline{\mathbb{F}}_{p^k}$.

Prerequisites (3/3)

We say some $x \in R$ is a *unit* if $xy = 1 = yx$ for some $y \in R$. Denote $R^\times = \{x \in R \mid x \text{ is a unit.}\}$. Then $R^\times$ is a group, and $1 \in R^\times$.

Proposition

For any finite field $\mathbb{F}_{p^k}$, the group $\mathbb{F}_{p^k}^\times = \mathbb{F}_{p^k} \setminus \{0\}$ is *cyclic*, i.e. it is isomorphic to $\mathbb{Z}/(p^k - 1)\mathbb{Z}$. In fact, $x^{p^k} = x \iff x \in \mathbb{F}_{p^k} \subset \overline{\mathbb{F}}_{p^k}$.

Ideals

An *ideal* $I \subset R$ satisfies for any $x \in R$ and any $a \in I$, that $x \cdot a \in I$.

Prerequisites (3/3)

We say some $x \in R$ is a *unit* if $xy = 1 = yx$ for some $y \in R$. Denote $R^\times = \{x \in R \mid x \text{ is a unit.}\}$. Then $R^\times$ is a group, and $1 \in R^\times$.

Proposition

For any finite field $\mathbb{F}_{p^k}$, the group $\mathbb{F}_{p^k}^\times = \mathbb{F}_{p^k} \setminus \{0\}$ is *cyclic*, i.e. it is isomorphic to $\mathbb{Z}/(p^k - 1)\mathbb{Z}$. In fact, $x^{p^k} = x \iff x \in \mathbb{F}_{p^k} \subset \overline{\mathbb{F}}_{p^k}$.

Ideals

An *ideal* $I \subset R$ satisfies for any $x \in R$ and any $a \in I$, that $x \cdot a \in I$.

- The subset $2 \cdot \mathbb{Z} = \{2, 4, 6, \ldots\} \subset \mathbb{Z}$ is an ideal.

Prerequisites (3/3)

We say some $x \in R$ is a *unit* if $xy = 1 = yx$ for some $y \in R$. Denote $R^\times = \{x \in R \mid x \text{ is a unit.}\}$. Then $R^\times$ is a group, and $1 \in R^\times$.

Proposition

For any finite field $\mathbb{F}_{p^k}$, the group $\mathbb{F}_{p^k}^\times = \mathbb{F}_{p^k} \setminus \{0\}$ is *cyclic*, i.e. it is isomorphic to $\mathbb{Z}/(p^k - 1)\mathbb{Z}$. In fact, $x^{p^k} = x \iff x \in \mathbb{F}_{p^k} \subset \overline{\mathbb{F}}_{p^k}$.

Ideals

An *ideal* $I \subset R$ satisfies for any $x \in R$ and any $a \in I$, that $x \cdot a \in I$.

- The subset $2 \cdot \mathbb{Z} = \{2, 4, 6, \dots\} \subset \mathbb{Z}$ is an ideal.
- More generally, if $x \in R$, the ideal $I = x \cdot R$ denotes the set $\{x \cdot y \mid y \in R\}$. We say that I is *principal*.

Prerequisites (3/3)

We say some $x \in R$ is a *unit* if $xy = 1 = yx$ for some $y \in R$. Denote $R^\times = \{x \in R \mid x \text{ is a unit.}\}$. Then $R^\times$ is a group, and $1 \in R^\times$.

Proposition

For any finite field $\mathbb{F}_{p^k}$, the group $\mathbb{F}_{p^k}^\times = \mathbb{F}_{p^k} \setminus \{0\}$ is *cyclic*, i.e. it is isomorphic to $\mathbb{Z}/(p^k - 1)\mathbb{Z}$. In fact, $x^{p^k} = x \iff x \in \mathbb{F}_{p^k} \subset \overline{\mathbb{F}}_{p^k}$.

Ideals

An *ideal* $I \subset R$ satisfies for any $x \in R$ and any $a \in I$, that $x \cdot a \in I$.

- The subset $2 \cdot \mathbb{Z} = \{2, 4, 6, \ldots\} \subset \mathbb{Z}$ is an ideal.
- More generally, if $x \in R$, the ideal $I = x \cdot R$ denotes the set $\{x \cdot y \mid y \in R\}$. We say that I is *principal*. Not every ideal is principal; for example $I = \{f \in \mathbb{Z}[X] \mid f(0) \text{ is even}\}$.

Prerequisites (3/3)

We say some $x \in R$ is a *unit* if $xy = 1 = yx$ for some $y \in R$. Denote $R^\times = \{x \in R \mid x \text{ is a unit.}\}$. Then $R^\times$ is a group, and $1 \in R^\times$.

Proposition

For any finite field $\mathbb{F}_{p^k}$, the group $\mathbb{F}_{p^k}^\times = \mathbb{F}_{p^k} \setminus \{0\}$ is *cyclic*, i.e. it is isomorphic to $\mathbb{Z}/(p^k - 1)\mathbb{Z}$. In fact, $x^{p^k} = x \iff x \in \mathbb{F}_{p^k} \subset \overline{\mathbb{F}}_{p^k}$.

Ideals

An *ideal* $I \subset R$ satisfies for any $x \in R$ and any $a \in I$, that $x \cdot a \in I$.

- The subset $2 \cdot \mathbb{Z} = \{2, 4, 6, \ldots\} \subset \mathbb{Z}$ is an ideal.
- More generally, if $x \in R$, the ideal $I = x \cdot R$ denotes the set $\{x \cdot y \mid y \in R\}$. We say that I is *principal*. Not every ideal is principal; for example $I = \{f \in \mathbb{Z}[X] \mid f(0) \text{ is even}\}$.
- If every ideal in R is principal and R is a domain, we say that R is a *principal ideal domain*, or p.i.d. **Example:** $\mathbb{Z}$ is a p.i.d., $\mathbb{Z}[X]$ is not.

Backstory

A very easy exercise in a first course on group theory:

Problem

Let G be a group. Prove that the following are equivalent:

- G is abelian;
- For all $a, b \in G$, it holds that $(ab)^{-1} = a^{-1}b^{-1}$;
- For all $a, b \in G$, it holds that $(ab)^2 = a^2b^2$.

These problems are quite boring.

Backstory

A very easy exercise in a first course on group theory:

Problem

Let G be a group. Prove that the following are equivalent:

- G is abelian;
- For all $a, b \in G$, it holds that $(ab)^{-1} = a^{-1}b^{-1}$;
- For all $a, b \in G$, it holds that $(ab)^2 = a^2b^2$.

These problems are quite boring. More interesting is:

Proposition

Suppose that $a^2 = 1$ for all $a \in G$. Then G is abelian.

Proof: We see that $(ab)^2 = 1$, so $abab = 1$. Hence

$$ab = a(abab)b = ba,$$

where we used that also $a^2 = b^2 = 1$. □

The bridge

Proposition

Suppose that $a^2 = 1$ for all $a \in G$. Then G is abelian.

There are two reasons why this result is interesting:

- We used the given not just once, but *three* times.
- The result does not generalise, i.e. the group

$$G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, x, y, z \in \mathbb{Z}/3\mathbb{Z} \right\}$$

satisfies the property that $a^3 = 1$ for all $a \in G$, but G is not abelian.

The bridge

Proposition

Suppose that $a^2 = 1$ for all $a \in G$. Then G is abelian.

There are two reasons why this result is interesting:

- We used the given not just once, but *three* times.
- The result does not generalise, i.e. the group

$$G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \middle| \, x, y, z \in \mathbb{Z}/3\mathbb{Z} \right\}$$

satisfies the property that $a^3 = 1$ for all $a \in G$, but G is not abelian.

So, *something* must be going on.

Question: How do we suitably generalise this result to *rings*?

Failed attempt

Clearly $x^2 = 1$ cannot hold for all $x \in R$, because $0^2 = 1$ forces $R = \{0\}$.
What happens if we exclude 0?

Failed attempt

Clearly $x^2 = 1$ cannot hold for all $x \in R$, because $0^2 = 1$ forces $R = \{0\}$. What happens if we exclude 0?

Proposition

Let R be a ring in which $x^2 = 1$ for all $x \neq 0$. Then $R \cong \mathbb{F}_2$ or $R \cong \mathbb{F}_3$.

Failed attempt

Clearly $x^2 = 1$ cannot hold for all $x \in R$, because $0^2 = 1$ forces $R = \{0\}$. What happens if we exclude 0?

Proposition

Let R be a ring in which $x^2 = 1$ for all $x \neq 0$. Then $R \cong \mathbb{F}_2$ or $R \cong \mathbb{F}_3$.

Proof: We split two cases.

- Suppose that $2 = 0$ and let $x \in R \setminus \{0, 1\}$. Then

  $$1 = (x + 1)^2 = x^2 + 2x + 1 = 1 + 0 + 1 = 0,$$

  a contradiction. Hence $R = \mathbb{F}_2$.

Failed attempt

Clearly $x^2 = 1$ cannot hold for all $x \in R$, because $0^2 = 1$ forces $R = \{0\}$. What happens if we exclude 0?

Proposition

Let R be a ring in which $x^2 = 1$ for all $x \neq 0$. Then $R \cong \mathbb{F}_2$ or $R \cong \mathbb{F}_3$.

Proof: We split two cases.

- Suppose that $2 = 0$ and let $x \in R \setminus \{0, 1\}$. Then

$$1 = (x+1)^2 = x^2 + 2x + 1 = 1 + 0 + 1 = 0,$$

  a contradiction. Hence $R = \mathbb{F}_2$.

- Suppose that $2 \neq 0$. Then $2^2 = 1$, so $3 = 0$. Let $x \in R \setminus \{0, 1, 2\}$. Then

$$1 = (x+1)^2 = 1 - x + 1,$$

  so $x = 1$; a contradiction. Hence $R = \mathbb{F}_3$. □

The proper generalisation

So $x^2 = 1$ for all $x \neq 0$ is too much. Sadly, only considering $x \in R^\times$ is not enough, for consider

$$R = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \,\middle|\, x, y, z \in \mathbb{Z}/2\mathbb{Z} \right\}.$$

The two units square to 1, but the ring is not commutative.

The proper generalisation

So $x^2 = 1$ for all $x \neq 0$ is too much. Sadly, only considering $x \in R^\times$ is not enough, for consider

$$R = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \,\middle|\, x, y, z \in \mathbb{Z}/2\mathbb{Z} \right\}.$$

The two units square to 1, but the ring is not commutative.
The right way to generalise the result on groups is as follows:

Proposition

Suppose $x^2 = x$ holds for all $x \in R$. Then R is commutative.

Proof: First observe that $1 = (-1)^2 = -1$. Hence

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

We see that $xy + yx = 0$, and so $xy = -yx = yx$. □
These rings are called *boolean*.

It generalises further

There are again two reasons why this result is interesting:

- We again used the given not just once, but *four* times.
- The result *does* in fact generalise!

It generalises further

There are again two reasons why this result is interesting:

- We again used the given not just once, but *four* times.
- The result *does* in fact generalise!

Proposition

Suppose $x^3 = x$ holds for all $x \in R$. Then R is commutative.

There are multiple ways to prove this, but the shortest ones all rely on the following lemma.

It generalises further

There are again two reasons why this result is interesting:

- We again used the given not just once, but *four* times.
- The result *does* in fact generalise!

Proposition

Suppose $x^3 = x$ holds for all $x \in R$. Then R is commutative.

There are multiple ways to prove this, but the shortest ones all rely on the following lemma.

Lemma

Let R be a reduced ring and $e \in R$ an idempotent. Then e is central.

Proof: Let $x \in R$ be arbitrary. Then observe that

$$(exe - ex)^2 = exexe - exex - exexe + exex = 0.$$

Hence by assumption, $exe = ex$. Completely analogously, $ex = exe = xe$, showing that e is indeed central. □

Proving the proposition

Proposition

Suppose $x^3 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Clearly R is reduced, and $x^4 = x^2$, so that all squares in R must be central by the lemma. We now compute that:

Proving the proposition

Proposition

Suppose $x^3 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Clearly R is reduced, and $x^4 = x^2$, so that all squares in R must be central by the lemma. We now compute that:

$$\begin{aligned} xy &= (xy)^3 \\ &= x(yx)^2y \\ &= yxyx^2y \\ &= yx^3y^2 \\ &= y^3x \\ &= yx. \end{aligned}$$

□

Proving the proposition

Proposition

Suppose $x^3 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Clearly R is reduced, and $x^4 = x^2$, so that all squares in R must be central by the lemma. We now compute that:

$$\begin{aligned} xy &= (xy)^3 \\ &= x(yx)^2y \\ &= yxyx^2y \\ &= yx^3y^2 \\ &= y^3x \\ &= yx. \end{aligned}$$

What about even higher exponents? □

Another explicit example

Proposition

Suppose $x^4 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Again we have that $1 = (-1)^4 = -1$. We then compute that

$$(x^2 + x)^2 = x^4 + 2x^3 + x^2 = x^2 + x.$$

Hence $x^2 + x$ is an idempotent in the reduced ring R, which is thus central by the lemma.

Another explicit example

Proposition

Suppose $x^4 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Again we have that $1 = (-1)^4 = -1$. We then compute that

$$(x^2 + x)^2 = x^4 + 2x^3 + x^2 = x^2 + x.$$

Hence $x^2 + x$ is an idempotent in the reduced ring R, which is thus central by the lemma. Hence also

$$(x + y)^2 + (x + y) = (x^2 + x) + xy + yx + (y^2 + y)$$

is central, and as such, $xy + yx$ must be central for all $x, y \in R$.

Another explicit example

Proposition

Suppose $x^4 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Again we have that $1 = (-1)^4 = -1$. We then compute that

$$(x^2 + x)^2 = x^4 + 2x^3 + x^2 = x^2 + x.$$

Hence $x^2 + x$ is an idempotent in the reduced ring R, which is thus central by the lemma. Hence also

$$(x+y)^2 + (x+y) = (x^2 + x) + xy + yx + (y^2 + y)$$

is central, and as such, $xy + yx$ must be central for all $x, y \in R$.
In particular, we find that

$$xyx + yx^2 = (xy + yx)x = x(xy + yx) = x^2y + xyx,$$

and hence $yx^2 = x^2y$ for all $x, y \in R$. In other words, also x^2 is central, and thus so is $x = (x^2 + x) - x^2$. □

We power through...

Proposition

Suppose $x^5 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Note that $(x^4)^2 = x^5 \cdot x^3 = x^4$, so x^4 is an idempotent in the reduced ring R, hence central. We see that

$$(x+1)^4 \in Z(R) \implies 4x^3 + 6x^2 + 4x \in Z(R);$$
$$(x-1)^4 \in Z(R) \implies 4x^3 - 6x^2 + 4x \in Z(R).$$

Subtracting these two results gives that $12x^2 \in Z(R)$ for all $x \in R$.

We power through...

Proposition

Suppose $x^5 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Note that $(x^4)^2 = x^5 \cdot x^3 = x^4$, so x^4 is an idempotent in the reduced ring R, hence central. We see that

$$(x+1)^4 \in Z(R) \implies 4x^3 + 6x^2 + 4x \in Z(R);$$
$$(x-1)^4 \in Z(R) \implies 4x^3 - 6x^2 + 4x \in Z(R).$$

Subtracting these two results gives that $12x^2 \in Z(R)$ for all $x \in R$. Hence also

$$12(x+1)^2 \in Z(R) \implies 24x \in Z(R).$$

We power through...

Proposition

Suppose $x^5 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Note that $(x^4)^2 = x^5 \cdot x^3 = x^4$, so x^4 is an idempotent in the reduced ring R, hence central. We see that

$$(x+1)^4 \in Z(R) \implies 4x^3 + 6x^2 + 4x \in Z(R);$$
$$(x-1)^4 \in Z(R) \implies 4x^3 - 6x^2 + 4x \in Z(R).$$

Subtracting these two results gives that $12x^2 \in Z(R)$ for all $x \in R$. Hence also

$$12(x+1)^2 \in Z(R) \implies 24x \in Z(R).$$

But $2^5 = 2$ implies $30 = 0$ so also $6x \in Z(R)$.

We power through...

Proposition

Suppose $x^5 = x$ holds for all $x \in R$. Then R is commutative.

Proof: Note that $(x^4)^2 = x^5 \cdot x^3 = x^4$, so x^4 is an idempotent in the reduced ring R, hence central. We see that

$$(x+1)^4 \in Z(R) \implies 4x^3 + 6x^2 + 4x \in Z(R);$$
$$(x-1)^4 \in Z(R) \implies 4x^3 - 6x^2 + 4x \in Z(R).$$

Subtracting these two results gives that $12x^2 \in Z(R)$ for all $x \in R$. Hence also

$$12(x+1)^2 \in Z(R) \implies 24x \in Z(R).$$

But $2^5 = 2$ implies $30 = 0$ so also $6x \in Z(R)$. So

$$4x^3 + 6x^2 + 4x \in Z(R) \implies 2x^3 + 2x \in Z(R).$$

We power through...

Proposition

Suppose $x^5 = x$ holds for all $x \in R$. Then R is commutative.

Proof (cont.): Now consider

$$(x+1)^5 = x+1 \implies 10x^3 + 10x^2 + 5x \in Z(R);$$
$$(x-1)^5 = x-1 \implies 10x^3 - 10x^2 + 5x \in Z(R).$$

Adding these two results gives that $20x^3 + 10x \in Z(R)$ for all $x \in R$.
Hence also $2x^3 + 4x \in Z(R)$.

We power through...

Proposition

Suppose $x^5 = x$ holds for all $x \in R$. Then R is commutative.

Proof (cont.): Now consider

$$(x+1)^5 = x+1 \implies 10x^3 + 10x^2 + 5x \in Z(R);$$
$$(x-1)^5 = x-1 \implies 10x^3 - 10x^2 + 5x \in Z(R).$$

Adding these two results gives that $20x^3 + 10x \in Z(R)$ for all $x \in R$. Hence also $2x^3 + 4x \in Z(R)$. Recall that $2x^3 + 2x \in Z(R)$ for all $x \in R$. Combining this, we obtain $2x \in Z(R)$ for all $x \in R$.

We power through...

Proposition

Suppose $x^5 = x$ holds for all $x \in R$. Then R is commutative.

Proof (cont.): Now consider

$$(x+1)^5 = x+1 \implies 10x^3 + 10x^2 + 5x \in Z(R);$$
$$(x-1)^5 = x-1 \implies 10x^3 - 10x^2 + 5x \in Z(R).$$

Adding these two results gives that $20x^3 + 10x \in Z(R)$ for all $x \in R$. Hence also $2x^3 + 4x \in Z(R)$. Recall that $2x^3 + 2x \in Z(R)$ for all $x \in R$. Combining this, we obtain $2x \in Z(R)$ for all $x \in R$. Hence

$$10x^3 + 10x^2 + 5x \in Z(R) \implies 5x \in Z(R).$$

Hence also $x \in Z(R)$, completing the proof. □

A curious case

Proposition

Suppose $x^6 = x$ holds for all $x \in R$. Then R is commutative.

Proof: We start by remarking that once again, $2 = 0$. Now, writing out that $(x+1)^6 = x+1$ gives that

$$x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 = x + 1.$$

A curious case

Proposition

Suppose $x^6 = x$ holds for all $x \in R$. Then R is commutative.

Proof: We start by remarking that once again, $2 = 0$. Now, writing out that $(x+1)^6 = x+1$ gives that

$$x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 = x + 1.$$

In other words, $x^4 = x^2$ for all $x \in R$.

A curious case

Proposition

Suppose $x^6 = x$ holds for all $x \in R$. Then R is commutative.

Proof: We start by remarking that once again, $2 = 0$. Now, writing out that $(x+1)^6 = x+1$ gives that

$$x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 = x + 1.$$

In other words, $x^4 = x^2$ for all $x \in R$. Hence

$$x = x^6 = x^4 \cdot x^2 = x^2 \cdot x^2 = x^4 = x^2.$$

Hence R is boolean and in particular commutative. □

A curious case

Proposition

Suppose $x^6 = x$ holds for all $x \in R$. Then R is commutative.

Proof: We start by remarking that once again, $2 = 0$. Now, writing out that $(x+1)^6 = x+1$ gives that

$$x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 = x + 1.$$

In other words, $x^4 = x^2$ for all $x \in R$. Hence

$$x = x^6 = x^4 \cdot x^2 = x^2 \cdot x^2 = x^4 = x^2.$$

Hence R is boolean and in particular commutative. □

Observation

Suppose $x^6 = x$ holds for all $x \in R$. Then even $x^2 = x$ for all $x \in R$.

Secretly boolean?

Question 1

When are rings in which $x^n = x$ for all x secretly boolean?

Secretly boolean?

Question 1

When are rings in which $x^n = x$ for all x secretly boolean?

Question 2

What are all relations we can deduce from 1 variable for even n?

Secretly boolean?

Question 1

When are rings in which $x^n = x$ for all x secretly boolean?

Question 2

What are all relations we can deduce from 1 variable for even n?

For any $x \in R$ and $f \in \mathbb{F}_2[X]$, we have that $f(x)^n = f(x)$. So we define

$$I_n \subset \mathbb{F}_2[X] \quad \text{generated by} \quad f(X)^n - f(X) \quad \text{for all} \quad f \in \mathbb{F}_2[X].$$

Secretly boolean?

Question 1

When are rings in which $x^n = x$ for all x secretly boolean?

Question 2

What are all relations we can deduce from 1 variable for even n?

For any $x \in R$ and $f \in \mathbb{F}_2[X]$, we have that $f(x)^n = f(x)$. So we define

$$I_n \subset \mathbb{F}_2[X] \quad \text{generated by} \quad f(X)^n - f(X) \quad \text{for all} \quad f \in \mathbb{F}_2[X].$$

Proposition

The ring $\mathbb{F}_2[X]$ is a principal ideal domain.

Secretly boolean?

Question 1

When are rings in which $x^n = x$ for all x secretly boolean?

Question 2

What are all relations we can deduce from 1 variable for even n?

For any $x \in R$ and $f \in \mathbb{F}_2[X]$, we have that $f(x)^n = f(x)$. So we define

$$I_n \subset \mathbb{F}_2[X] \quad \text{generated by} \quad f(X)^n - f(X) \quad \text{for all} \quad f \in \mathbb{F}_2[X].$$

Proposition

The ring $\mathbb{F}_2[X]$ is a principal ideal domain.

Corollary

There exists some $g_n \in \mathbb{F}_2[X]$ such that $I_n = (g_n)$.

Secretly boolean?

Question 1

When are rings in which $x^n = x$ for all x secretly boolean?

Question 2

What are all relations we can deduce from 1 variable for even n?

For any $x \in R$ and $f \in \mathbb{F}_2[X]$, we have that $f(x)^n = f(x)$. So we define

$$I_n \subset \mathbb{F}_2[X] \quad \text{generated by} \quad f(X)^n - f(X) \quad \text{for all} \quad f \in \mathbb{F}_2[X].$$

Proposition

The ring $\mathbb{F}_2[X]$ is a principal ideal domain.

Corollary

There exists some $g_n \in \mathbb{F}_2[X]$ such that $I_n = (g_n)$.

Then g_n is the *minimal relation*. Can we determine it?

Example

Let's re-examine the exponent 6 case in this language. By definition:

$$(x+1)^6 - (x+1) \in I_6 \implies x^4 + x^2 \in I_6.$$

Example

Let's re-examine the exponent 6 case in this language. By definition:

$$(x+1)^6 - (x+1) \in I_6 \implies x^4 + x^2 \in I_6.$$

Then also

$$x^2 \cdot (x^4 + x^2) = x^6 + x^4 \in I_6.$$

Example

Let's re-examine the exponent 6 case in this language. By definition:

$$(x+1)^6 - (x+1) \in I_6 \implies x^4 + x^2 \in I_6.$$

Then also

$$x^2 \cdot (x^4 + x^2) = x^6 + x^4 \in I_6.$$

By definition, we also have

$$x^6 + x \in I_6.$$

Example

Let's re-examine the exponent 6 case in this language. By definition:

$$(x+1)^6 - (x+1) \in I_6 \implies x^4 + x^2 \in I_6.$$

Then also

$$x^2 \cdot (x^4 + x^2) = x^6 + x^4 \in I_6.$$

By definition, we also have

$$x^6 + x \in I_6.$$

But then also

$$(x + x^6) + (x^6 + x^4) + (x^4 + x^2) = x^2 + x \in I_6.$$

This means that $I_6 = (x^2 + x)$. Can we do this in general?

The main result

Theorem

Define the set $S_n = \{m \in \mathbb{N} : 2^m - 1 \mid n - 1\}$. Then we have

$$g_n = \operatorname{lcm}\left\{X^{2^m} - X \mid m \in S_n\right\}.$$

The main result

Theorem

Define the set $S_n = \{m \in \mathbb{N} : 2^m - 1 \mid n - 1\}$. Then we have

$$g_n = \operatorname{lcm}\left\{X^{2^m} - X \mid m \in S_n\right\}.$$

- If $n = 2$ then $S_n = \{1\}$ so $g_n = X^2 - X$.
- If $n = 4$ then $S_n = \{1, 2\}$ so $g_n = X^4 - X$.
- If $n = 6$ then $S_n = \{1\}$ so $g_n = X^2 - X$.
- If $n = 8$ then $S_n = \{1, 3\}$ so $g_n = X^8 - X$.
- If $n = 10$ then $S_n = \{1, 2\}$ so $g_n = X^4 - X$.
- If $n = 12$ then $S_n = \{1\}$ so $g_n = X^2 - X$.
- If $n = 14$ then $S_n = \{1\}$ so $g_n = X^2 - X$.
- If $n = 16$ then $S_n = \{1, 2, 4\}$ so $g_n = X^{16} - X$.
- If $n = 18$ then $S_n = \{1\}$ so $g_n = X^2 - X$.
- If $n = 20$ then $S_n = \{1\}$ so $g_n = X^2 - X$.
- If $n = 22$ then $S_n = \{1, 2, 3\}$ so $g_n = (X^2 + X + 1)(X^8 - X)$.
- If $n = 24$ then $S_n = \{1\}$ so $g_n = X^2 - X$.

Proof part 1/2

Theorem

Define the set $S_n = \{m \in \mathbb{N} : 2^m - 1 \mid n - 1\}$. Then we have

$$g_n = \operatorname{lcm}\left\{X^{2^m} - X \mid m \in S_n\right\}.$$

Proof: Two (squarefree) polynomials over $\mathbb{F}_2$ are equal if and only if they have the same zeroes in $\overline{\mathbb{F}}_2$.

Proof part 1/2

Theorem

Define the set $S_n = \{m \in \mathbb{N} : 2^m - 1 \mid n - 1\}$. Then we have

$$g_n = \operatorname{lcm}\left\{X^{2^m} - X \mid m \in S_n\right\}.$$

Proof: Two (squarefree) polynomials over $\mathbb{F}_2$ are equal if and only if they have the same zeroes in $\overline{\mathbb{F}}_2$.

- Zeroes of the RHS: if and only if it is a zero of $X^{2^m} - X$ for some $m \in S_n$. Equivalently, if and only if $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$.

Proof part 1/2

Theorem

Define the set $S_n = \{m \in \mathbb{N} : 2^m - 1 \mid n - 1\}$. Then we have

$$g_n = \text{lcm}\left\{X^{2^m} - X \mid m \in S_n\right\}.$$

Proof: Two (squarefree) polynomials over $\mathbb{F}_2$ are equal if and only if they have the same zeroes in $\overline{\mathbb{F}}_2$.

- Zeroes of the RHS: if and only if it is a zero of $X^{2^m} - X$ for some $m \in S_n$. Equivalently, if and only if $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$.
- Zeroes of the LHS: if and only if it is a zero of all $h^n - h$ for $h \in \mathbb{F}_2[X]$. We have thus reduced to showing that for $\alpha \in \overline{\mathbb{F}}_2$,

$$h(\alpha)^n = h(\alpha) \text{ for all } h \in \mathbb{F}_2[X] \iff \alpha \in \mathbb{F}_{2^m} \text{ for some } m \in S_n.$$

Proof part 2/2

$$h(\alpha)^n = h(\alpha) \text{ for all } h \in \mathbb{F}_2[X] \iff \alpha \in \mathbb{F}_{2^m} \text{ for some } m \in S_n.$$

Proof part 2/2

$$h(\alpha)^n = h(\alpha) \text{ for all } h \in \mathbb{F}_2[X] \iff \alpha \in \mathbb{F}_{2^m} \text{ for some } m \in S_n.$$

- Let $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$. If $h(\alpha) = 0$, we are done.

Proof part 2/2

$$h(\alpha)^n = h(\alpha) \text{ for all } h \in \mathbb{F}_2[X] \iff \alpha \in \mathbb{F}_{2^m} \text{ for some } m \in S_n.$$

- Let $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$. If $h(\alpha) = 0$, we are done. If $h(\alpha) \in \mathbb{F}_{2^m}^\times$, then $h(\alpha)^{2^m-1} = 1$. By definition of m, raising this to some power yields that $h(\alpha)^{n-1} = 1$, as desired.

Proof part 2/2

$$h(\alpha)^n = h(\alpha) \text{ for all } h \in \mathbb{F}_2[X] \iff \alpha \in \mathbb{F}_{2^m} \text{ for some } m \in S_n.$$

- Let $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$. If $h(\alpha) = 0$, we are done. If $h(\alpha) \in \mathbb{F}_{2^m}^\times$, then $h(\alpha)^{2^m-1} = 1$. By definition of m, raising this to some power yields that $h(\alpha)^{n-1} = 1$, as desired.
- Now let $\alpha \in \overline{\mathbb{F}}_2$ and suppose that $h(\alpha)^n = h(\alpha)$ for all $h \in \mathbb{F}_2[X]$. If we write $\mathbb{F}_2[\alpha] = \mathbb{F}_{2^m}$ for some $m \in \mathbb{N}$, we must show that $m \in S_n$.

Proof part 2/2

$$h(\alpha)^n = h(\alpha) \text{ for all } h \in \mathbb{F}_2[X] \iff \alpha \in \mathbb{F}_{2^m} \text{ for some } m \in S_n.$$

- Let $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$. If $h(\alpha) = 0$, we are done. If $h(\alpha) \in \mathbb{F}_{2^m}^\times$, then $h(\alpha)^{2^m-1} = 1$. By definition of m, raising this to some power yields that $h(\alpha)^{n-1} = 1$, as desired.
- Now let $\alpha \in \overline{\mathbb{F}}_2$ and suppose that $h(\alpha)^n = h(\alpha)$ for all $h \in \mathbb{F}_2[X]$. If we write $\mathbb{F}_2[\alpha] = \mathbb{F}_{2^m}$ for some $m \in \mathbb{N}$, we must show that $m \in S_n$. Observe that

$$\{h(\alpha) \mid h \in \mathbb{F}_2[X]\} = \mathbb{F}_2[\alpha] = \mathbb{F}_{2^m}.$$

Proof part 2/2

$$h(\alpha)^n = h(\alpha) \text{ for all } h \in \mathbb{F}_2[X] \iff \alpha \in \mathbb{F}_{2^m} \text{ for some } m \in S_n.$$

- Let $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$. If $h(\alpha) = 0$, we are done. If $h(\alpha) \in \mathbb{F}_{2^m}^\times$, then $h(\alpha)^{2^m-1} = 1$. By definition of m, raising this to some power yields that $h(\alpha)^{n-1} = 1$, as desired.
- Now let $\alpha \in \overline{\mathbb{F}}_2$ and suppose that $h(\alpha)^n = h(\alpha)$ for all $h \in \mathbb{F}_2[X]$. If we write $\mathbb{F}_2[\alpha] = \mathbb{F}_{2^m}$ for some $m \in \mathbb{N}$, we must show that $m \in S_n$. Observe that

$$\{h(\alpha) \mid h \in \mathbb{F}_2[X]\} = \mathbb{F}_2[\alpha] = \mathbb{F}_{2^m}.$$

In other words, $\beta^n = \beta$ for all $\beta \in \mathbb{F}_{2^m}$. Since $\mathbb{F}_{2^m}^\times$ is cyclic of order $2^m - 1$, we may choose β to be a generator. It then follows immediately that $2^m - 1 \mid n - 1$, showing $m \in S_n$. □

How many cases can we solve?

Question

When are rings in which $x^n = x$ for all x secretly boolean?

How many cases can we solve?

Question

When are rings in which $x^n = x$ for all x secretly boolean?

Answer

Precisely when $n - 1$ is not divisible by any $2^m - 1$ for $m \geqslant 2$.

How many cases can we solve?

Question

When are rings in which $x^n = x$ for all x secretly boolean?

Answer

Precisely when $n - 1$ is not divisible by any $2^m - 1$ for $m \geqslant 2$.

Question

How many rings in which $x^n = x$ for all x are secretly boolean?

How many cases can we solve?

Question

When are rings in which $x^n = x$ for all x secretly boolean?

Answer

Precisely when $n - 1$ is not divisible by any $2^m - 1$ for $m \geqslant 2$.

Question

How many rings in which $x^n = x$ for all x are secretly boolean?

Lemma

Let $m, n \in \mathbb{N}$. Then $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(m,n)} - 1$.

How many cases can we solve?

Question

When are rings in which $x^n = x$ for all x secretly boolean?

Answer

Precisely when $n - 1$ is not divisible by any $2^m - 1$ for $m \geqslant 2$.

Question

How many rings in which $x^n = x$ for all x are secretly boolean?

Lemma

Let $m, n \in \mathbb{N}$. Then $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(m,n)} - 1$.

- $n - 1$ is not divisible by any $2^m - 1$ as soon as $n - 1$ is not divisible by any $2^p - 1$ for p prime. *Example:* not divisible by $2^3 - 1 = 7$ implies also not divisible by $2^6 - 1 = 63$.

How many cases can we solve?

Question

When are rings in which $x^n = x$ for all x secretly boolean?

Answer

Precisely when $n - 1$ is not divisible by any $2^m - 1$ for $m \geqslant 2$.

Question

How many rings in which $x^n = x$ for all x are secretly boolean?

Lemma

Let $m, n \in \mathbb{N}$. Then $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(m,n)} - 1$.

- $n - 1$ is not divisible by any $2^m - 1$ as soon as $n - 1$ is not divisible by any $2^p - 1$ for p prime. *Example:* not divisible by $2^3 - 1 = 7$ implies also not divisible by $2^6 - 1 = 63$.
- For primes $p \neq q$, the numbers $2^p - 1$ and $2^q - 1$ are coprime.

Densities and probabilities

Theorem

The density of even n for which any ring R in which $x^n = x$ for all $x \in R$ is necessarily boolean is given by

$$\alpha := \prod_{p \text{ prime}} \frac{2^p - 2}{2^p - 1} \approx 0.54830.$$

Densities and probabilities

Theorem

The density of even n for which any ring R in which $x^n = x$ for all $x \in R$ is necessarily boolean is given by

$$\alpha := \prod_{p \text{ prime}} \frac{2^p - 2}{2^p - 1} \approx 0.54830.$$

Proof: The probability of *not* being divisible by $2^p - 1$ for a prime p is equal to

$$1 - \frac{1}{2^p - 1} = \frac{2^p - 2}{2^p - 1}.$$

Densities and probabilities

Theorem

The density of even n for which any ring R in which $x^n = x$ for all $x \in R$ is necessarily boolean is given by

$$\alpha := \prod_{p \text{ prime}} \frac{2^p - 2}{2^p - 1} \approx 0.54830.$$

Proof: The probability of *not* being divisible by $2^p - 1$ for a prime p is equal to

$$1 - \frac{1}{2^p - 1} = \frac{2^p - 2}{2^p - 1}.$$

Since all these numbers are coprime, these events are independent. □

Corollary

Using just the techniques from this presentation, we can prove commutativity for a density of $7\alpha/5 \approx 0.76762$ of even exponents.

Our achievements

The following table summarises for which values of n, we can prove that any ring satisfying $x^n = x$ must be commutative:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Comm?	✓	✓	✓	✓	✓	?	?	?	✓	?	✓	?	✓	?

Our achievements

The following table summarises for which values of n, we can prove that any ring satisfying $x^n = x$ must be commutative:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Comm?	✓	✓	✓	✓	✓	?	?	?	✓	?	✓	?	✓	?

For even exponents our results are even better:

n	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Comm?	✓	✓	✓	?	✓	✓	✓	?	✓	✓	?	✓	✓	✓	✓

Our achievements

The following table summarises for which values of n, we can prove that any ring satisfying $x^n = x$ must be commutative:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Comm?	✓	✓	✓	✓	✓	?	?	?	✓	?	✓	?	✓	?

For even exponents our results are even better:

n	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Comm?	✓	✓	✓	?	✓	✓	✓	?	✓	✓	?	✓	✓	✓	✓

Question: is it true in general?

Our achievements

The following table summarises for which values of n, we can prove that any ring satisfying $x^n = x$ must be commutative:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Comm?	✓	✓	✓	✓	✓	?	?	?	✓	?	✓	?	✓	?

For even exponents our results are even better:

n	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Comm?	✓	✓	✓	?	✓	✓	✓	?	✓	✓	?	✓	✓	✓	✓

Question: is it true in general? **Answer:** Much more is true!

Our achievements

The following table summarises for which values of n, we can prove that any ring satisfying $x^n = x$ must be commutative:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Comm?	✓	✓	✓	✓	✓	?	?	?	✓	?	✓	?	✓	?

For even exponents our results are even better:

n	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Comm?	✓	✓	✓	?	✓	✓	✓	?	✓	✓	?	✓	✓	✓	✓

Question: is it true in general? **Answer:** Much more is true!

Theorem (Jacobson)

Let R be a ring in which for any $x \in R$ there exists some integer $n(x) \geqslant 2$ such that $x^{n(x)} = x$. Then R is commutative.

Our achievements

The following table summarises for which values of n, we can prove that any ring satisfying $x^n = x$ must be commutative:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Comm?	✓	✓	✓	✓	✓	?	?	?	✓	?	✓	?	✓	?

For even exponents our results are even better:

n	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Comm?	✓	✓	✓	?	✓	✓	✓	?	✓	✓	?	✓	✓	✓	✓

Question: is it true in general? **Answer:** Much more is true!

Theorem (Jacobson)

Let R be a ring in which for any $x \in R$ there exists some integer $n(x) \geqslant 2$ such that $x^{n(x)} = x$. Then R is commutative.

So why look for these kinds of proofs? Because it's fun!

Our achievements

The following table summarises for which values of n, we can prove that any ring satisfying $x^n = x$ must be commutative:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Comm?	✓	✓	✓	✓	✓	?	?	?	✓	?	✓	?	✓	?

For even exponents our results are even better:

n	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Comm?	✓	✓	✓	?	✓	✓	✓	?	✓	✓	?	✓	✓	✓	✓

Question: is it true in general? **Answer:** Much more is true!

Theorem (Jacobson)

Let R be a ring in which for any $x \in R$ there exists some integer $n(x) \geqslant 2$ such that $x^{n(x)} = x$. Then R is commutative.

So why look for these kinds of proofs? Because it's fun! (to me)

Our achievements

The following table summarises for which values of n, we can prove that any ring satisfying $x^n = x$ must be commutative:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Comm?	✓	✓	✓	✓	✓	?	?	?	✓	?	✓	?	✓	?

For even exponents our results are even better:

n	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Comm?	✓	✓	✓	?	✓	✓	✓	?	✓	✓	?	✓	✓	✓	✓

Question: is it true in general? **Answer:** Much more is true!

Theorem (Jacobson)

Let R be a ring in which for any $x \in R$ there exists some integer $n(x) \geqslant 2$ such that $x^{n(x)} = x$. Then R is commutative.

So why look for these kinds of proofs? Because it's fun! (to me)

Thanks for listening!