Jacobson's Commutativity Theorem

Mike Daas

Universiteit Leiden

June 18, 2021

Universiteit Leiden

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

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

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*?
For us, a ring will always have 1.

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 $xy = -yx = yx$. □

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 mutliple 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 mutliple 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 can now finish in three ways:

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 can now finish in three ways:

A. By purely multiplying,

$$xy = (xy)^3 = x(yx)^2y = yxyx^2y = yx^3y^2 = y^3x = yx.$$

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 can now finish in three ways:

A. By purely multiplying,

$$xy = (xy)^3 = x(yx)^2y = yxyx^2y = yx^3y^2 = y^3x = yx.$$

B. Alternatively, consider $x^2 + x$ and compute that

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

Hence $x^2 + x = (x^2 + x)^3 = 2(x^2 + x)^2$ is central, and thus x too.

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 can now finish in three ways:

A. By purely multiplying,

$$xy = (xy)^3 = x(yx)^2y = yxyx^2y = yx^3y^2 = y^3x = yx.$$

B. Alternatively, consider $x^2 + x$ and compute that

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

Hence $x^2 + x = (x^2 + x)^3 = 2(x^2 + x)^2$ is central, and thus x too.

C. Yet alternatively, note that $2x = (x^2 + x)^2 - 2x^2$ must be central, and that since

$$x + 1 = (x + 1)^3 = x^3 + 3x^2 + 3x + 1 = x + 1 + 3(x^2 + x)$$

it follows that $3x = -3x^2$ must be central, and $x = 3x - 2x$. □

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 $x = (x^2 + x) - x^2$. □

Infinite famlies I

Proposition

Let $n \geqslant 0$ be an integer and suppose that $x^{3\cdot 2^n} = x$ holds for all $x \in R$. Then R is commutative.

Proof: We discussed $n = 0$. If $n \geqslant 1$, we again have that $-1 = 1$ and hence we find that

$$x + 1 = (x+1)^{3\cdot 2^n} = (x^{2^n} + 1)^3 = x^{3\cdot 2^n} + x^{2\cdot 2^n} + x^{2^n} + 1.$$

We conclude that $x^{2\cdot 2^n} = x^{2^n}$ for all $x \in R$, and hence $x^2 = (x^2)^{3\cdot 2^n} = (x^3)^{2\cdot 2^n} = (x^3)^{2^n} = x$ so R is in fact Boolean. □

Infinite famlies I

Proposition

Let $n \geqslant 0$ be an integer and suppose that $x^{3\cdot 2^n} = x$ holds for all $x \in R$. Then R is commutative.

Proof: We discussed $n = 0$. If $n \geqslant 1$, we again have that $-1 = 1$ and hence we find that

$$x + 1 = (x+1)^{3\cdot 2^n} = (x^{2^n} + 1)^3 = x^{3\cdot 2^n} + x^{2\cdot 2^n} + x^{2^n} + 1.$$

We conclude that $x^{2\cdot 2^n} = x^{2^n}$ for all $x \in R$, and hence $x^2 = (x^2)^{3\cdot 2^n} = (x^3)^{2\cdot 2^n} = (x^3)^{2^n} = x$ so R is in fact Boolean. □

Proposition

Let $n \geqslant 1$ be an integer and suppose that $x^{5\cdot 2^n} = x$ holds for all $x \in R$. Then R is commutative.

Proof: Exactly the same as before, but since $(x+1)^5 \equiv x^5 + x^4 + x + 1 \mod 2$, we reduce to the solved $x^4 = x$. Note we exclude $n = 0$. □

Infinite families II

Lemma

Let $m \geqslant 0$ be an integer. Then the only odd entries in the $2^m + 1$-th row of Pascal's triangle are precisely the two 1's and the two $2^m + 1$'s. □

Proposition (D., 2021)

Let $m \geqslant 1$ be an integer. Suppose that any ring R in which $x^{2^m} = x$ for all $x \in R$ must be commutative. Then the same must hold for rings in which $x^{(2^m+1)\cdot 2^n} = x$ for all $x \in R$ for any integer $n \geqslant 1$.

Infinite families II

Lemma

Let $m \geqslant 0$ be an integer. Then the only odd entries in the $2^m + 1$-th row of Pascal's triangle are precisely the two 1's and the two $2^m + 1$'s. □

Proposition (D., 2021)

Let $m \geqslant 1$ be an integer. Suppose that any ring R in which $x^{2^m} = x$ for all $x \in R$ must be commutative. Then the same must hold for rings in which $x^{(2^m+1)\cdot 2^n} = x$ for all $x \in R$ for any integer $n \geqslant 1$.

Proof: We use the above lemma to write that

$$x + 1 = (x+1)^{(2^m+1)\cdot 2^n} = (x^{2^n} + 1)^{2^m+1} = x^{(2^m+1)\cdot 2^n} + x^{2^m \cdot 2^n} + x^{2^n} + 1.$$

Hence $x^{2^m \cdot 2^n} = x^{2^n}$ for all $x \in R$, and as such,

$$x^{2^m} = (x^{2^m})^{(2^m+1)\cdot 2^n} = (x^{2^m+1})^{2^m \cdot 2^n} = (x^{2^m+1})^{2^n} = x.$$

This establishes our reduction. □

Infinite famlies III

Proposition (D., 2021)

Let $n, m \geqslant 1$ be a integers such that there is no odd prime p such that $2^n \equiv 2^m \equiv (p+1)/2 \mod p$. Suppose that $x^{2^n+2^m} = x$ holds for all $x \in R$. Then R is Boolean and hence commutative.

Infinite famlies III

Proposition (D., 2021)

Let $n, m \geqslant 1$ be a integers such that there is no odd prime p such that $2^n \equiv 2^m \equiv (p+1)/2 \mod p$. Suppose that $x^{2^n+2^m} = x$ holds for all $x \in R$. Then R is Boolean and hence commutative.

Proof: We proceed along the same lines, by writing

$$\begin{aligned} x+1 &= (x+1)^{2^n+2^m} = (x+1)^{2^n}(x+1)^{2^m} = (x^{2^n}+1)(x^{2^m}+1) \\ &= x^{2^n+2^m} + x^{2^n} + x^{2^m} + 1. \end{aligned}$$

It follows that $x^{2^n} = x^{2^m}$ for all $x \in R$, and so $x = x^{2^n+2^m} = x^{2^{m+1}}$.

Infinite famlies III

Proposition (D., 2021)

Let $n, m \geqslant 1$ be a integers such that there is no odd prime p such that $2^n \equiv 2^m \equiv (p+1)/2 \mod p$. Suppose that $x^{2^n+2^m} = x$ holds for all $x \in R$. Then R is Boolean and hence commutative.

Proof: We proceed along the same lines, by writing

$$\begin{aligned} x+1 &= (x+1)^{2^n+2^m} = (x+1)^{2^n}(x+1)^{2^m} = (x^{2^n}+1)(x^{2^m}+1) \\ &= x^{2^n+2^m} + x^{2^n} + x^{2^m} + 1. \end{aligned}$$

It follows that $x^{2^n} = x^{2^m}$ for all $x \in R$, and so $x = x^{2^n+2^m} = x^{2^{m+1}}$. We may thus consider the exponent modulo $2^{m+1}-1$, whereas on the other hand we may write that $x = x^{2^n+2^m} = x^{1+k\cdot(2^n+2^m-1)}$ for all integers $k \geqslant 0$. The assumption on n and m is such that $2^n + 2^m - 1$ and $2^{m+1}-1$ are coprime,

Infinite famlies III

Proposition (D., 2021)

Let $n, m \geqslant 1$ be a integers such that there is no odd prime p such that $2^n \equiv 2^m \equiv (p+1)/2 \mod p$. Suppose that $x^{2^n+2^m} = x$ holds for all $x \in R$. Then R is Boolean and hence commutative.

Proof: We proceed along the same lines, by writing

$$\begin{aligned} x+1 &= (x+1)^{2^n+2^m} = (x+1)^{2^n}(x+1)^{2^m} = (x^{2^n}+1)(x^{2^m}+1) \\ &= x^{2^n+2^m} + x^{2^n} + x^{2^m} + 1. \end{aligned}$$

It follows that $x^{2^n} = x^{2^m}$ for all $x \in R$, and so $x = x^{2^n+2^m} = x^{2^{m+1}}$. We may thus consider the exponent modulo $2^{m+1}-1$, whereas on the other hand we may write that $x = x^{2^n+2^m} = x^{1+k\cdot(2^n+2^m-1)}$ for all integers $k \geqslant 0$. The assumption on n and m is such that $2^n + 2^m - 1$ and $2^{m+1}-1$ are coprime, so that we can find some k such that

$$1 + k \cdot (2^n + 2^m - 1) \equiv 2 \mod 2^{m+1} - 1.$$

It follows that $x = x^2$, and so R is Boolean. □

What we managed so far

Remark: The proof strategy above shows something slightly stronger: if $1 + k \cdot (2^n + 2^m - 1)$ can agree modulo $2^{m+1} - 1$ with any exponent for which we already know R must be commutative, then the result follows for the exponent $2^n + 2^m$ as well by reduction.

What we managed so far

Remark: The proof strategy above shows something slightly stronger: if $1 + k \cdot (2^n + 2^m - 1)$ can agree modulo $2^{m+1} - 1$ with any exponent for which we already know R must be commutative, then the result follows for the exponent $2^n + 2^m$ as well by reduction.
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?	✓	✓	✓	?	✓	?	?	?	✓	?	✓	?	?	?

n	16	17	18	19	20	21	22	23	24	25	26	27
Comm?	?	?	✓	?	✓	?	?	?	✓	?	?	?

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

What we managed so far

Remark: The proof strategy above shows something slightly stronger: if $1 + k \cdot (2^n + 2^m - 1)$ can agree modulo $2^{m+1} - 1$ with any exponent for which we already know R must be commutative, then the result follows for the exponent $2^n + 2^m$ as well by reduction.
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?	✓	✓	✓	?	✓	?	?	?	✓	?	✓	?	?	?

n	16	17	18	19	20	21	22	23	24	25	26	27
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.

Proof sketch I

Herstein's Lemma

Let D be a division ring of characteristic $p > 0$. Let a be a non-central torsion element of $D^\times$. Then there exists some additive commutator $y \in D^\times$ such that $yay^{-1} = a^i \neq a$ for some $i > 0$.

Proof: (sketch) Let $\delta_a : x \mapsto ax - xa$ be the derivation associated with a and let $K = \mathbb{F}_p[a]$. Then K is a finite field by assumption on which δ_a vanishes, but $\delta_a \neq 0$ on D as a K-linear operator. One can show that δ_a has an eigenvector with eigenvalue in $K^\times$, so write $ax - xa = bx$ for some $b \in K^\times$. This really is the hard work.

Proof sketch I

Herstein's Lemma

Let D be a division ring of characteristic $p > 0$. Let a be a non-central torsion element of $D^\times$. Then there exists some additive commutator $y \in D^\times$ such that $yay^{-1} = a^i \neq a$ for some $i > 0$.

Proof: (sketch) Let $\delta_a : x \mapsto ax - xa$ be the derivation associated with a and let $K = \mathbb{F}_p[a]$. Then K is a finite field by assumption on which δ_a vanishes, but $\delta_a \neq 0$ on D as a K-linear operator. One can show that δ_a has an eigenvector with eigenvalue in $K^\times$, so write $ax - xa = bx$ for some $b \in K^\times$. This really is the hard work.
In the cyclic group $K^\times$, the elements $xax^{-1} = a - b \in K \setminus \{a\}$ and a have the same order and hence generate the same subgroup, from which we find $xax^{-1} = a^i \neq a$. Then

$$(ax - xa)a = aa^ix - a^ixa = a^i(ax - xa),$$

as claimed. □

Proof sketch II

Theorem

Let D be a division ring in which for every $x, y \in D$, there exists some integer $n(x,y) \geqslant 2$ such that $(xy - yx)^{n(x,y)} = xy - yx$.
Then D is a field.

Proof: Write F for the centre of D. Then F is a field, and we claim that every element in F has finite order. Indeed, for $c \in F$, also $c(xy - yx) = (cx)y - y(cx)$ is an additive commutator, and so for some integer n,

$$c^n(xy - yx)^n = 1 = (xy - yx)^n,$$

whence $c^n = 1$. It follows that $\mathrm{char}(F) = \mathrm{char}(D) > 0$.

Proof sketch II

Theorem

Let D be a division ring in which for every $x, y \in D$, there exists some integer $n(x,y) \geqslant 2$ such that $(xy - yx)^{n(x,y)} = xy - yx$.
Then D is a field.

Proof: Write F for the centre of D. Then F is a field, and we claim that every element in F has finite order. Indeed, for $c \in F$, also $c(xy - yx) = (cx)y - y(cx)$ is an additive commutator, and so for some integer n,

$$c^n(xy - yx)^n = 1 = (xy - yx)^n,$$

whence $c^n = 1$. It follows that $\mathrm{char}(F) = \mathrm{char}(D) > 0$. Let $a \in D \setminus F$. Then Herstein's Lemma gives us some additive commutator $y \in D^\times$ such that $yay^{-1} = a^i \neq a$ for some $i > 0$.

Proof sketch II

Theorem

Let D be a division ring in which for every $x, y \in D$, there exists some integer $n(x,y) \geqslant 2$ such that $(xy - yx)^{n(x,y)} = xy - yx$.
Then D is a field.

Proof: Write F for the centre of D. Then F is a field, and we claim that every element in F has finite order. Indeed, for $c \in F$, also $c(xy - yx) = (cx)y - y(cx)$ is an additive commutator, and so for some integer n,

$$c^n(xy - yx)^n = 1 = (xy - yx)^n,$$

whence $c^n = 1$. It follows that $\mathrm{char}(F) = \mathrm{char}(D) > 0$. Let $a \in D \setminus F$. Then Herstein's Lemma gives us some additive commutator $y \in D^\times$ such that $yay^{-1} = a^i \neq a$ for some $i > 0$. Since y is also torsion in $D^\times$ and y normalises $\langle a \rangle$, it follows that $\langle a \rangle \cdot \langle y \rangle$ is a finite subgroup of $D^\times$. The $\mathbb{F}_p$-span of this subgroup is a finite subring of D, and thus by Wedderburn's Theorem, it must be a field, i.e. commutative. But $yay^{-1} \neq a$; a contradiction. □

Proof sketch III

Definition

A ring R is called *left-primitive* it is has a simple faithful left-module.

Proof sketch III

Definition

A ring R is called *left-primitive* it is has a simple faithful left-module.

Structure theorem for left-primitive rings

Let R be a left-primitive ring. Then either $R \cong M_n(D)$ for some integer $n \geqslant 1$ and division ring D, or for any integer $n \geqslant 1$, there is a subring R_n of R that maps onto $M_n(D)$.

Proof sketch III

Definition

A ring R is called *left-primitive* it is has a simple faithful left-module.

Structure theorem for left-primitive rings

Let R be a left-primitive ring. Then either $R \cong M_n(D)$ for some integer $n \geqslant 1$ and division ring D, or for any integer $n \geqslant 1$, there is a subring R_n of R that maps onto $M_n(D)$.

Theorem

Let R be left-primitive with for every $x, y \in R$ some integer $n(x, y) \geqslant 2$ such that $(xy - yx)^{n(x,y)} = xy - yx$. Then R is commutative.

Proof: Note that $a = E_{11}$ and $b = E_{12}$ in $M_n(D)$ for $n \geqslant 2$ satisfy $(ab - ba)^n = b^n = 0$, so it cannot satisfy the condition above. Hence the second possibility from the structure theorem cannot hold, and the first can only hold for $n = 1$; that is, $R \cong M_1(D) = D$. □

Proof sketch IV

We continue to expand our class of rings for which we know the Jacobson-Herstein theorem to hold.

Definition

A ring R is called *semi-primitive* if its Jacobson radical is 0. Equivalently, if R has a semisimple faithful (left-)module.

Proof sketch IV

We continue to expand our class of rings for which we know the Jacobson-Herstein theorem to hold.

Definition

A ring R is called *semi-primitive* if its Jacobson radical is 0. Equivalently, if R has a semisimple faithful (left-)module.

Definition

We say R is a *subdirect product* of some family of rings $\{R_i\}_{i\in I}$ if there exists an injective ring morphism $R \to \prod_{i\in I} R_i$ such that each of the induced maps $R \to R_i$ is surjective.

Proof sketch IV

We continue to expand our class of rings for which we know the Jacobson-Herstein theorem to hold.

Definition

A ring R is called *semi-primitive* if its Jacobson radical is 0. Equivalently, if R has a semisimple faithful (left-)module.

Definition

We say R is a *subdirect product* of some family of rings $\{R_i\}_{i\in I}$ if there exists an injective ring morphism $R \to \prod_{i\in I} R_i$ such that each of the induced maps $R \to R_i$ is surjective.

Theorem

A ring R is semiprimitive if and only if it is a subdirect product of left primitive rings.

Proof sketch V

Theorem

Let R be a semi-primitive ring in which for every $x, y \in R$, there exists some integer $n(x,y) \geqslant 2$ such that $(xy - yx)^{n(x,y)} = xy - yx$.
Then R is commutative.

Proof: Consider any subdirect product representation $R \to \prod R_i$, where all of the R_i are left-primitive rings. Since each projection is surjective, each of the R_i must satisfy the conditions from the theorem, and hence by our previous efforts, must be commutative. Since R injects into $\prod R_i$, we may view it as a subring of this commutative ring. Hence it must also be commutative. □

Proof sketch V

Theorem

Let R be a semi-primitive ring in which for every $x, y \in R$, there exists some integer $n(x,y) \geqslant 2$ such that $(xy - yx)^{n(x,y)} = xy - yx$.
Then R is commutative.

Proof: Consider any subdirect product representation $R \to \prod R_i$, where all of the R_i are left-primitive rings. Since each projection is surjective, each of the R_i must satisfy the conditions from the theorem, and hence by our previous efforts, must be commutative. Since R injects into $\prod R_i$, we may view it as a subring of this commutative ring. Hence it must also be commutative. □

We recall one fact about the Jacobson radical $\mathrm{rad}(R)$:

$$\mathrm{rad}(R) = \{x \in R \mid 1 + RxR \subset R^{\times}\}.$$

Proof sketch VI

Jacobson-Herstein Theorem

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

Proof: Let $\mathrm{rad}(R)$ denote the Jacobson radical of R. Then $R/\mathrm{rad}(R)$ also satisfies the conditions from the theorem and is semi-primitive, and hence must be commutative. Hence any commutator $z = xy - yx$ must fall inside $\mathrm{rad}(R)$. But $z^n = z$ for some n, and hence $z(1 - z^{n-1}) = 0$. However, since $1 - z^{n-1} \in 1 + \mathrm{rad}(R) \subset R^\times$, from this we see that $z = 0$. Hence R is commutative. □

Proof sketch VI

Jacobson-Herstein Theorem

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

Proof: Let $\mathrm{rad}(R)$ denote the Jacobson radical of R. Then $R/\mathrm{rad}(R)$ also satisfies the conditions from the theorem and is semi-primitive, and hence must be commutative. Hence any commutator $z = xy - yx$ must fall inside $\mathrm{rad}(R)$. But $z^n = z$ for some n, and hence $z(1 - z^{n-1}) = 0$. However, since $1 - z^{n-1} \in 1 + \mathrm{rad}(R) \subset R^\times$, from this we see that $z = 0$. Hence R is commutative. □

Question: So why bother with all our computations? The theorem is known in greater generality, so who cares?
Answer: Because it is fun! As we have seen, there are *elementary* proofs for these special cases. They are out there for any exponent. It would be interesting to find them, and to bypass all this machinery.

Jacobson's Theorem

It should be noted that a shorter proof of Jacobson's Theorem is possible, losing a tiny bit of generality.

Structure theorem for reduced rings

A ring R is reduced if and only if R is a subdirect product of domains.

Jacobson's Theorem

It should be noted that a shorter proof of Jacobson's Theorem is possible, losing a tiny bit of generality.

Structure theorem for reduced rings

A ring R is reduced if and only if R is a subdirect product of domains.

Jacobson's Theorem

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.

Proof: Realise R as a subring of $\prod_i D_i$, where the D_i are all integral domains. Since all projections are surjective, all the D_i must satisfy the same condition as R. But if $x^n = x$ in a domain, it follows that $x = 0$ or $x^{n-1} = 1$. It follows that D_i is even a division ring, hence commutative by our earlier efforts. □

Jacobson's Theorem

It should be noted that a shorter proof of Jacobson's Theorem is possible, losing a tiny bit of generality.

Structure theorem for reduced rings

A ring R is reduced if and only if R is a subdirect product of domains.

Jacobson's Theorem

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.

Proof: Realise R as a subring of $\prod_i D_i$, where the D_i are all integral domains. Since all projections are surjective, all the D_i must satisfy the same condition as R. But if $x^n = x$ in a domain, it follows that $x = 0$ or $x^{n-1} = 1$. It follows that D_i is even a division ring, hence commutative by our earlier efforts. □

There exist more such theorems, for example the Herstein-Kaplansky theorem. (See the book "A first course on noncommutative rings.")

The smallest open case

Proposition (D., 2021)

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

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

Adding these two results gives that $8x^3 + 8x \in Z(R)$ for all $x \in R$.

The smallest open case

Proposition (D., 2021)

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

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

Adding these two results gives that $8x^3 + 8x \in Z(R)$ for all $x \in R$. Subtracting these two results gives that $12x^2 \in Z(R)$ for all $x \in R$. Hence also

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

This is as much as we can deduce purely from the fact that fourth powers are central.

The smallest open case

Proposition (D., 2021)

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 $x \in R$.

The smallest open case

Proposition (D., 2021)

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 $x \in R$. Recall that $8x^3 + 8x \in Z(R)$ for all $x \in R$. Combining this, we obtain

$$5 \cdot (8x^3 + 8x) - 2 \cdot (20x^3 + 10x) \in Z(R) \implies 20x \in Z(R).$$

Recall that also $24x \in Z(R)$. Hence also $4x \in Z(R)$ for all $x \in R$.

The smallest open case

Proposition (D., 2021)

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 $x \in R$. Recall that $8x^3 + 8x \in Z(R)$ for all $x \in R$. Combining this, we obtain

$$5 \cdot (8x^3 + 8x) - 2 \cdot (20x^3 + 10x) \in Z(R) \implies 20x \in Z(R).$$

Recall that also $24x \in Z(R)$. Hence also $4x \in Z(R)$ for all $x \in R$. Hence

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

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

Thanks for listening!

Research questions:

- Can we write down an "elementary" proof or strategy for a general exponent?
- For which n are rings in which $x^n = x$ holds, necessarily *boolean*?

Exercises: If you are interested in messing around with rings with silly properties, try one of the following:

- Let $n \geqslant 1$ be an integer and suppose that $x^{n+1} = x^n$ for all $x \in R$. Show that R is Boolean. *(Medium.)*
- Let R be a ring in which $(xy)^2 = x^2y^2$ for all $x, y \in R$. Show that R is commutative. *(Hard.)*
- Generalise the above to higher exponents. *(Very hard!)*