**Modern Algebra and Number Systems**
**Lesson 7**
**Theorems about Groups**

***Warning: homework must be done following the methods taught in the videos. If not done this way, the feedback will simply be "watch the videos". Everyone will have exactly one opportunity to receive feedback and resubmit work. Don't waste that opportunity by not watching the videos.***

**Watch the Playlist 314F20-Lesson7 imagining that you have a private tutor (me) helping you read this chapter of the book and giving you as much time as you need to work each problem out before providing hints. Don't forget you can upload everything you've done and truly ask me for a hint at any time.**

11:03 PM Mon Aug 31

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra &... | Linear Algebra

Lesson 7

SECTION 3

# FUNDAMENTAL THEOREMS ABOUT GROUPS

**THEOREM 3.1 (Uniqueness of the identity element)** If $(G,*)$ is a group, then there is only one identity element in $G$.

*PROOF.* We must establish that if $e$ and $e_1$ are two elements of $G$ both of which satisfy the defining property of an identity element in $G$, then in fact $e=e_1$. That is, we *assume* that $x*e=e*x=x$ for *all* $x$ in $G$ *and* $x*e_1=e_1*x=x$ for *all* $x$ in $G$, and we then proceed to show that $e$ must equal $e_1$.

By the assumption on $e$, we have in particular (taking $x$ to be $e_1$)

$$e_1*e=e*e_1=e_1;$$

By the assumption on $e_1$, we have (taking $x$ to be $e$)

$$e*e_1=e_1*e=e.$$

Thus we have $e_1=e*e_1=e$, and the proof is complete. □

**THEOREM 3.2 (Uniqueness of inverses)** If $(G,*)$ is a group and $x$ is any element of $G$, then $x$ has only one inverse in $G$.

*PROOF.* We must show that if both $y_1$ and $y_2$ satisfy the definition of an inverse of $x$, that is, if $x*y_1=y_1*x=e$ and $x*y_2=y_2*x=e$, then in fact $y_1=y_2$.

25

Modern Algebra & Number Systems

Modern Algebra &... | Abstract_Algebra_1-5 | Linear Algebra

Lesson 7

**Defn**: A group $(G,*)$ is a set of elements $g\in G$ and a binary operation $*$

$\forall a,b\in G \quad a*b\in G$

that is associative

$\forall a,b,c\in G \quad a*(b*c)=(a*b)*c$

there is an identity $e\in G$

$\forall x\in G \quad e*x=x*e=x$

there are inverses in $G$

$\forall x\in G \quad \exists y\in G$ s.t

$x*y=y*x=e.$

11:04 PM Mon Aug 31

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra &... | Linear Algebra

Lesson 7

SECTION 3

# FUNDAMENTAL THEOREMS ABOUT GROUPS

**THEOREM 3.1 (Uniqueness of the identity element)** If $(G,*)$ is a group, then there is only one identity element in $G$.

*PROOF.* We must establish that if $e$ and $e_1$ are two elements of $G$ both of which satisfy the defining property of an identity element in $G$, then in fact $e=e_1$. That is, we *assume* that $x*e=e*x=x$ for *all* $x$ in $G$ *and* $x*e_1=e_1*x=x$ for *all* $x$ in $G$, and we then proceed to show that $e$ must equal $e_1$.

By the assumption on $e$, we have in particular (taking $x$ to be $e_1$)

$$e_1*e=e*e_1=e_1;$$

By the assumption on $e_1$, we have (taking $x$ to be $e$)

$$e*e_1=e_1*e=e.$$

Thus we have $e_1=e*e_1=e$, and the proof is complete. □

**THEOREM 3.2 (Uniqueness of inverses)** If $(G,*)$ is a group and $x$ is any element of $G$, then $x$ has only one inverse in $G$.

*PROOF.* We must show that if both $y_1$ and $y_2$ satisfy the definition of an inverse of $x$, that is, if $x*y_1=y_1*x=e$ and $x*y_2=y_2*x=e$, then in fact $y_1=y_2$.

25

53%

Modern Algebra & Number Systems

Modern Algebra &... | Abstract_Algebra_1-5 | Linear Algebra

Lesson 7

Defn: A group $(G,*)$ is a set of elements $g\in G$ and a binary operation $*$

$\forall a,b\in G \quad a*b\in G$

that is associative

$\forall a,b,c\in G \quad a*(b*c)=(a*b)*c$

there is an identity $e\in G$

$\forall x\in G \quad e*x=x*e=x$

there are inverses in $G$

$\forall x\in G \quad \exists y\in G$ s.t

$x*y=y*x=e.$

Try to write the proof of Theorem 1 with statements and justifications.

11:15 PM Mon Aug 31

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra &... | Linear Algebra

SECTION 3

Lesson 7

# FUNDAMENTAL THEOREMS ABOUT GROUPS

Defn A group $(G,*)$ is a set $G$ with a binary operation: $\forall a,b \in G \quad a*b \in G$ that is associative: $\forall a,b,c \in G \quad a*(b*c)=(a*b)*c$ has an identity element: $\exists e \in G$ s.t. $\forall x \in G \quad e*x=x*e=x$ and inverses: $\forall x \in G \ \exists y \in G$ s.t. $x*y=y*x=e$

**THEOREM 3.1 (Uniqueness of the identity element)** If $(G,*)$ is a group, then there is only one identity element in $G$.

*PROOF.* We must establish that if $e$ and $e_1$ are two elements of $G$ both of which satisfy the defining property of an identity element in $G$, then in fact $e=e_1$. That is, we *assume* that $x*e=e*x=x$ for *all* $x$ in $G$ *and* $x*e_1=e_1*x=x$ for *all* $x$ in $G$, and we then proceed to show that $e$ must equal $e_1$.

By the assumption on $e$, we have in particular (taking $x$ to be $e_1$)

$$e_1*e=e*e_1=e_1;$$

By the assumption on $e_1$, we have (taking $x$ to be $e$)

$$e*e_1=e_1*e=e.$$

Thus we have $e_1=e*e_1=e$, and the proof is complete. □

**THEOREM 3.2 (Uniqueness of inverses)** If $(G,*)$ is a group and $x$ is any element of $G$, then $x$ has only one inverse in $G$.

*PROOF.* We must show that if both $y_1$ and $y_2$ satisfy the definition of an inverse of $x$, that is, if $x*y_1=y_1*x=e$ and $x*y_2=y_2*x=e$, then in fact $y_1=y_2$.

25

51%

Modern Algebra & Number Systems

Modern Algebra &... | Abstract_Algebra_1-5 | Linear Algebra

Thm 3.1 : The identity element is unique (there is only one of them).

Examples All had unique Identity elements!

- $(\mathbb{Z}_p, +\bmod p)$ 0 was the identity $0+a=a+0=a$
- $(\mathbb{Q}_+, *)$ 1 was the identity $1\cdot\frac{p}{q}=\frac{p}{q}=1=\frac{p}{q}$ $\forall \frac{p}{q} \in \mathbb{Q}$
- $(GL(2,\mathbb{R}), \times)$ $Id=\begin{bmatrix}1&0\\0&1\end{bmatrix}$ $\begin{bmatrix}1&0\\0&1\end{bmatrix}\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}\begin{bmatrix}1&0\\0&1\end{bmatrix}=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}$

11:30 PM Mon Aug 31

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra &... | Linear Algebra

Lesson 7

SECTION 3

# FUNDAMENTAL THEOREMS ABOUT GROUPS

**Defn** A group $(G,*)$ is a set $G$ with a binary operation: $\forall a,b \in G \ a*b \in G$ that is associative: $\forall a,b,c \in G \ a*(b*c)=(a*b)*c$ has an identity element: $\exists e \in G$ s.t. $\forall x \in G \ e*x=x*e=x$ and inverses: $\forall x \in G \ \exists y \in G$ s.t. $x*y=y*x=e$

**THEOREM 3.1 (Uniqueness of the identity element)** If $(G,*)$ is a group, then there is only one identity element in $G$.

*PROOF.* We must establish that if $e$ and $e_1$ are two elements of $G$ both of which satisfy the defining property of an identity element in $G$, then in fact $e=e_1$. That is, we *assume* that $x*e=e*x=x$ for *all* $x$ in $G$ *and* $x*e_1=e_1*x=x$ for *all* $x$ in $G$, and we then proceed to show that $e$ must equal $e_1$.

By the assumption on $e$, we have in particular (taking $x$ to be $e_1$)

$$e_1*e=e*e_1=e_1;$$

By the assumption on $e_1$, we have (taking $x$ to be $e$)

$$e*e_1=e_1*e=e.$$

Thus we have $e_1=e*e_1=e$, and the proof is complete. □

**THEOREM 3.2 (Uniqueness of inverses)** If $(G,*)$ is a group and $x$ is any element of $G$, then $x$ has only one inverse in $G$.

*PROOF.* We must show that if both $y_1$ and $y_2$ satisfy the definition of an inverse of $x$, that is, if $x*y_1=y_1*x=e$ and $x*y_2=y_2*x=e$, then in fact $y_1=y_2$.

$\exists!$ means "there exists only one"

25

Modern Algebra & Number Systems

Modern Algebra &... | Abstract_Algebra_1-5 | Linear Algebra

**Thm 3.1**: The identity element is unique (there is only one of them).

$\exists! e \in G$ s.t. $\forall x \in G \ e*x=x*e=x$.

**Proof** by Contradiction:

1. Assume on the contrary that $\exists$ two identity elements $e$ and $e_1 \in G$ — (1) Indirect Hypothesis
2. $x*e=e*x=x \ \forall x \in G$ — (2) by step 1 $e$ is an identity element and defn of identity
3. $x*e_1=e_1*x=x \ \forall x \in G$ — (3) by step 1 $e_1$ is an identity element and defn of identity
4. $e_1*e=e*e_1=e_1$ — (4) Taking $x=e_1$ in step 2
5. $e*e_1=e_1*e=e$ — (5) Taking $x=e$ in step 3
6. $e_1=e*e_1=e$ — (6) by steps 4+5 and $a=b$ and $b=c \Rightarrow a=c$

⊗ They are the same. Not two!

Thus only one identity element

QED.

11:43 PM Mon Aug 31

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra &... | Linear Algebra

Thus we have $e_1 = e * e_1 = e$, and the proof is complete. □

**THEOREM 3.2 (Uniqueness of inverses)** If $(G, *)$ is a group and $x$ is any element of $G$, then $x$ has only one inverse in $G$.

*PROOF.* We must show that if both $y_1$ and $y_2$ satisfy the definition of an inverse of $x$, that is, if $x * y_1 = y_1 * x = e$ and $x * y_2 = y_2 * x = e$, then in fact $y_1 = y_2$.

Proof not yet done
Turn page





We will take some of the given information and use it to derive an equation which has $y_1$ on one side and $y_2$ on the other. It may leap to your eye, for example, that

$$x * y_1 = x * y_2,$$

because both sides are $e$. Once this is seen, all that remains is to get rid of the $x$'s. We can do this by using more of the given information, namely the fact that $y_1 * x = e$. We multiply both sides by $y_1$:

$$y_1 * (x * y_1) = y_1 * (x * y_2).$$

By using associativity, we get from this

$$\begin{aligned}(y_1 * x) * y_1 &= (y_1 * x) * y_2,\\ e * y_1 &= e * y_2,\\ y_1 &= y_2,\end{aligned}$$

as desired. ■

The proof is finished, but we are going to do it again in a slightly different way to illustrate the fact that there are often several different ways to prove something. Suppose, for example, that the equation $x * y_1 = x * y_2$ did *not* leap to your eye, and that you just took one of the equations given, say

$$y_1 * x = e,$$

to start with. If you want to get from this an equation with $y_1$ on one side and $y_2$ on the other, then certainly you observe that $y_1$ is already on the left, and we can get $y_2$ on the right by multiplying both sides by $y_2$:

$$\begin{aligned}(y_1 * x) * y_2 &= e * y_2\\ &= y_2.\end{aligned}$$

Now if only we could get rid of the $x$ and $y_2$ on the left-hand side, we'd be done, but we know from the equations we had to start with that $x * y_2 = e$, so we rewrite the left side by using associativity, so as to bring $x * y_2$ into play:

Modern Algebra & Number Systems

Modern Algebra &... | Abstract_Algebra_1-5 | Linear Algebra

**Thm 3.2 (Uniqueness of Inverses)**
If $(G,*)$ is a group and $x \in G$
then $\exists!\, y \in G$ s.t. $x*y = y*x = e$.
only one $y$

**Proof by Contradiction**

① Assume on the contrary that there are two inverses $y_1, y_2$ for an element $x \in G$

① by Indirect Hypothesis

② $x * y_1 = y_1 * x = e$ ② step 1 says $y_1$ is an inverse + defn of inverse

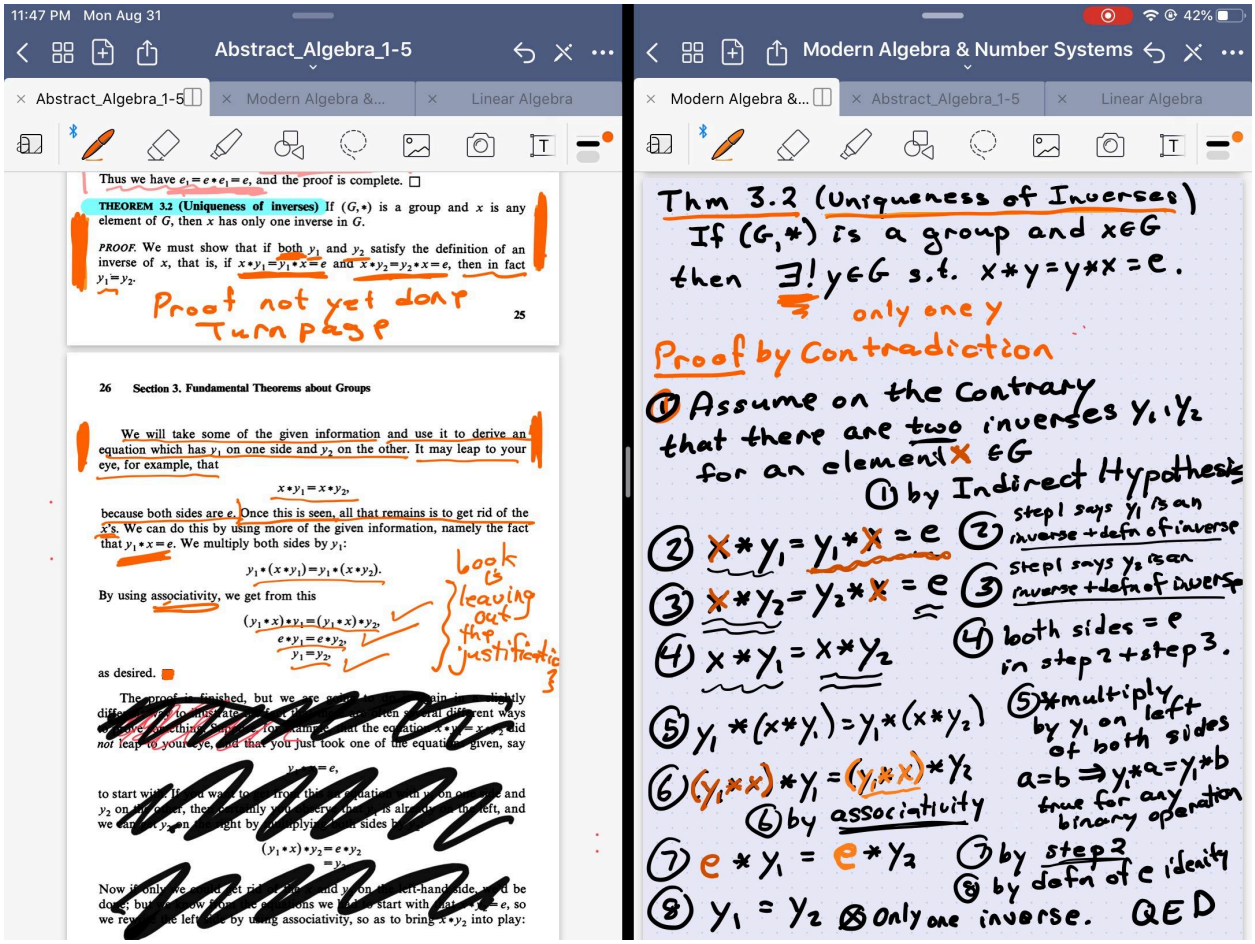
③ $x * y_2 = y_2 * x = e$ ③ step 1 says $y_2$ is an inverse + defn of inverse

④ $x * y_1 = x * y_2$ ④ both sides = e in step 2 + step 3.

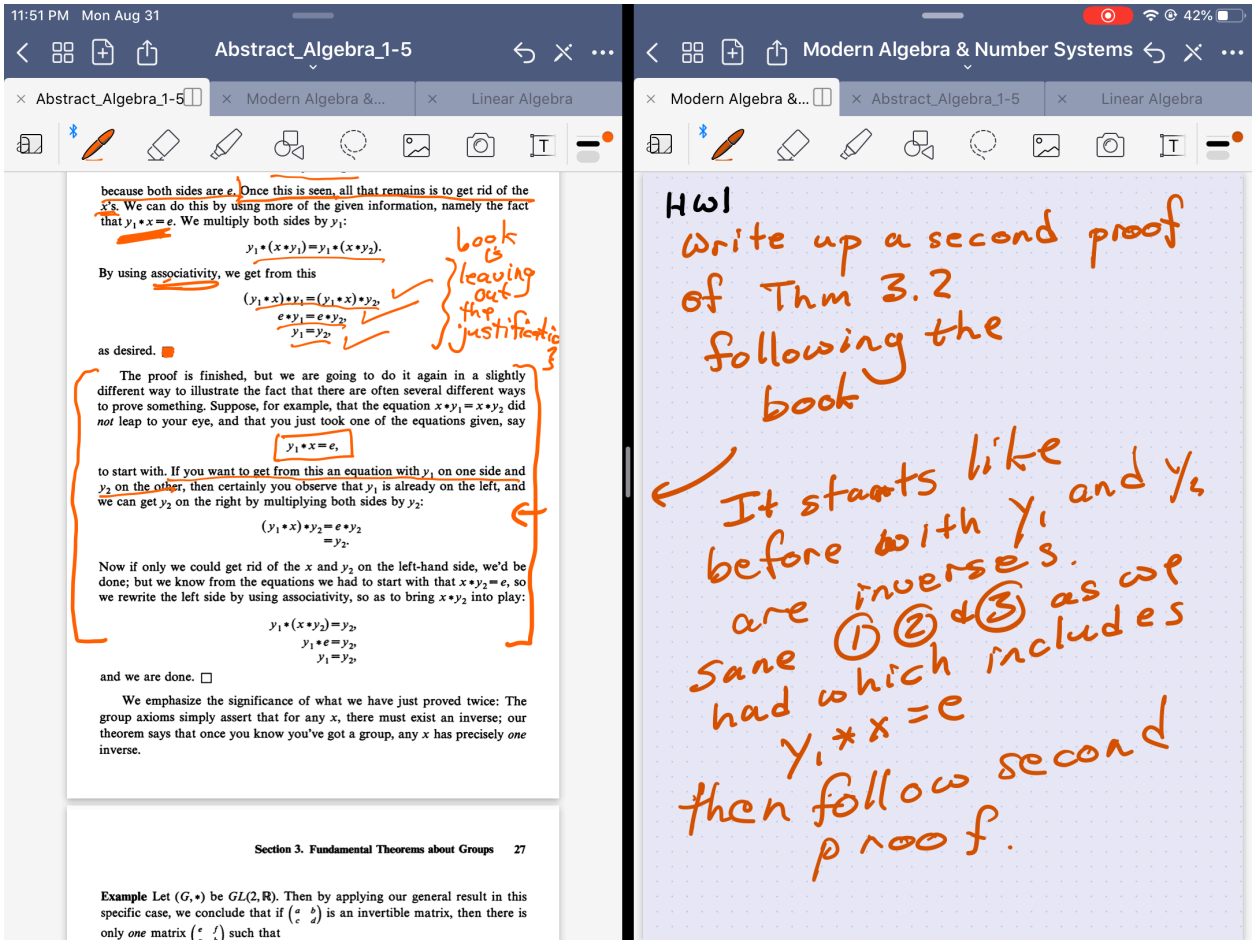
⑤ $y_1 * (x * y_1) = y_1 * (x * y_2)$ ⑤ *multiply by $y_1$ on left of both sides

$a = b \Rightarrow y_1 * a = y_1 * b$ true for any binary operation

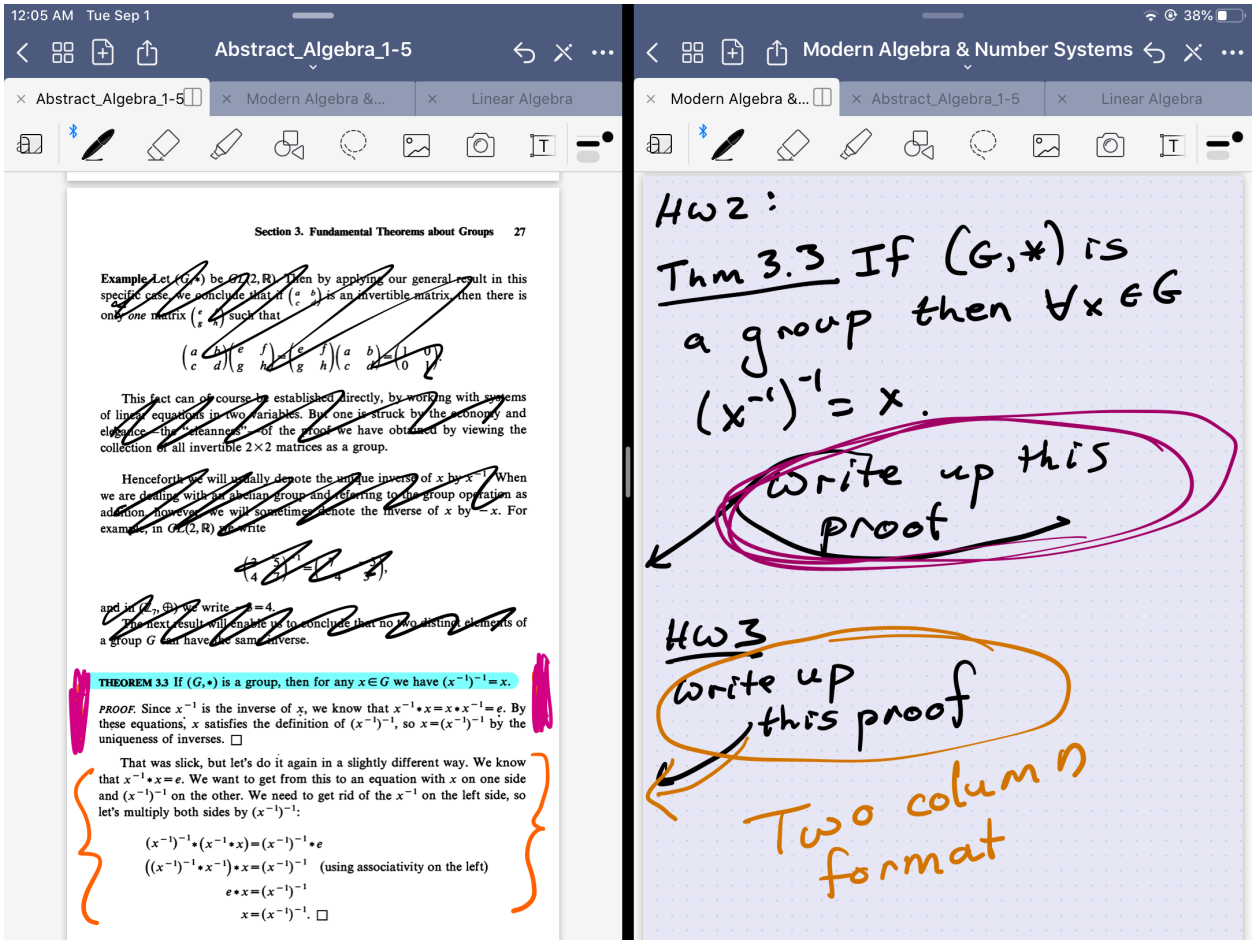
Cannot do
~~$y_1 * a = b * y_1$~~



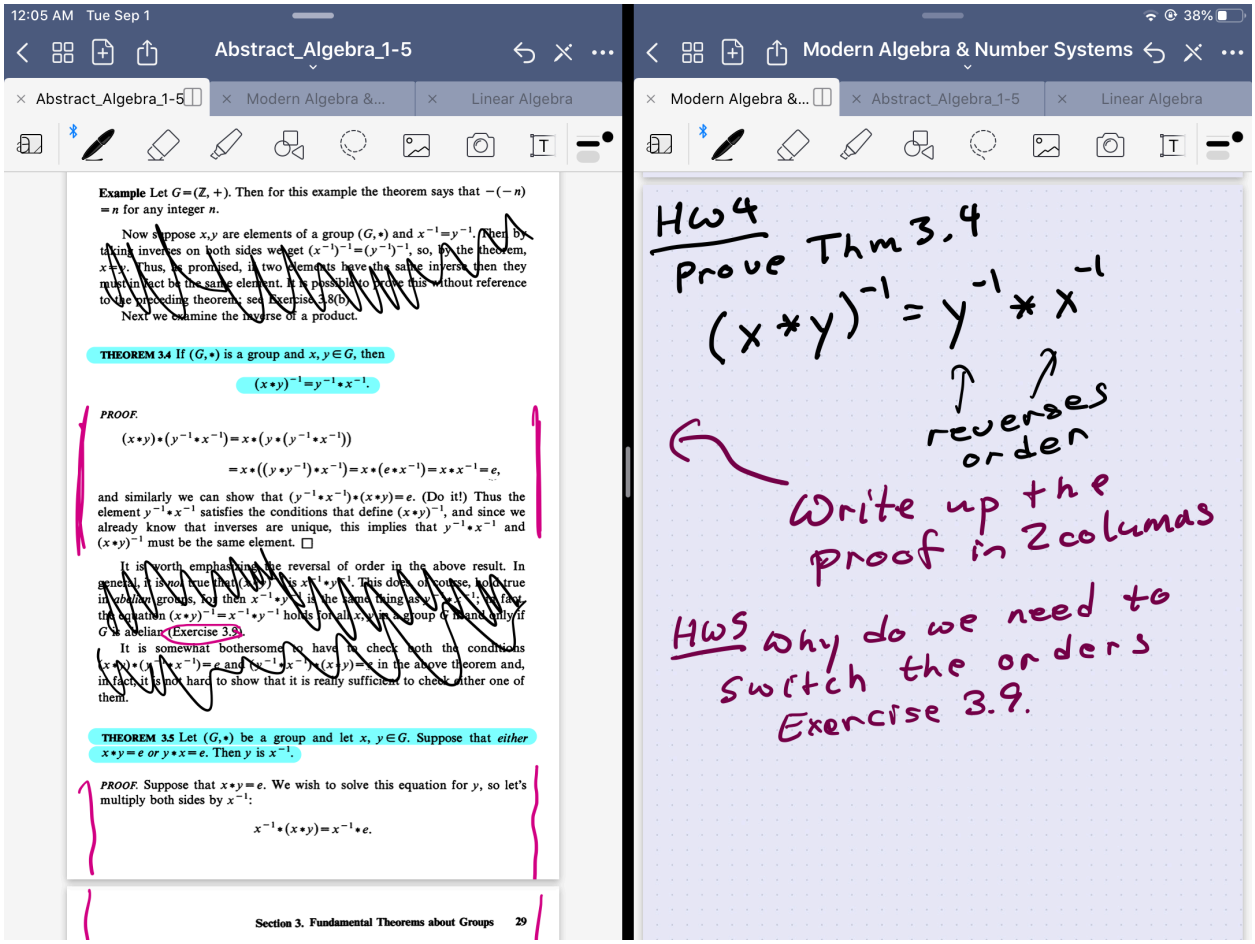

**HW1 is in here:**




**HW2 and HW3 are here: (if you are late you may skip HW2)**




**HW4 and HW5 are here: (if you are late you may skip HW5)**




**HW6 is in here:**

12:06 AM Tue Sep 1

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra &... | Linear Algebra

**THEOREM 3.4** If $(G,*)$ is a group and $x, y \in G$, then

$$(x*y)^{-1} = y^{-1}*x^{-1}.$$

*PROOF.*

$$(x*y)*(y^{-1}*x^{-1}) = x*(y*(y^{-1}*x^{-1}))$$

$$= x*((y*y^{-1})*x^{-1}) = x*(e*x^{-1}) = x*x^{-1} = e,$$

and similarly we can show that $(y^{-1}*x^{-1})*(x*y) = e$. (Do it!) Thus the element $y^{-1}*x^{-1}$ satisfies the conditions that define $(x*y)^{-1}$, and since we already know that inverses are unique, this implies that $y^{-1}*x^{-1}$ and $(x*y)^{-1}$ must be the same element. □

It is worth emphasizing the reversal of order in the above result. In general, it is *not* true that $(x*y)^{-1} = x^{-1}*y^{-1}$. This does, of course, hold true in *abelian* groups, for then $x^{-1}*y^{-1}$ is the same thing as $y^{-1}*x^{-1}$; in fact, the equation $(x*y)^{-1} = x^{-1}*y^{-1}$ holds for all $x, y$ in a group $G$ if and only if $G$ is abelian (Exercise 3.9).

It is somewhat bothersome to have to check both the conditions $(x*y)*(y^{-1}*x^{-1}) = e$ and $(y^{-1}*x^{-1})*(x*y) = e$ in the above theorem and, in fact, it is not hard to show that it is really sufficient to check either one of them.

**THEOREM 3.5** Let $(G,*)$ be a group and let $x, y \in G$. Suppose that *either* $x*y = e$ *or* $y*x = e$. Then $y$ is $x^{-1}$.

*PROOF.* Suppose that $x*y = e$. We wish to solve this equation for $y$, so let's multiply both sides by $x^{-1}$:

$$x^{-1}*(x*y) = x^{-1}*e.$$



Thus

$$(x^{-1}*x)*y = x^{-1},$$
$$e*y = x^{-1},$$
$$y = x^{-1}.$$

A similar argument shows that $y*x = e$ is also by itself sufficient to guarantee that $y = x^{-1}$. (Do it!) □

The same solving of an equation proves the more general

38%

Modern Algebra & Number Systems

Modern Algebra &... | Abstract_Algebra_1-5 | Linear Algebra

**Thm 3.5:**

If $(G,*)$ is a group and $x, y \in G$ if $x*y = e$ then $y = x^{-1}$

Also if $y*x = e$ then $y = x^{-1}$

You no longer have to check both sides.

HW6 is to write the proof in 2 columns.

The same solving of an equation proves the more general

**THEOREM 3.6 (Cancellation laws)** Let $(G,*)$ be a group and let $x, y, z \in G$. Then:

i) if $x*y = x*z$, then $y = z$; and

ii) if $y*x = z*x$, then $y = z$.

The proof is left as an exercise. Part (i) is called the **left cancellation law**, and part (ii) the **right cancellation law**.

We close this section by giving another formulation of the axioms for a group which is equivalent to our original definition but somewhat simpler to work with in establishing that some system is in fact a group.

**THEOREM 3.7** Let $G$ be a set and $*$ an associative binary operation on $G$. Assume that there is an element $e \in G$ such that $x*e = x$ for all $x \in G$, and assume that for any $x \in G$ there exists an element $y$ in $G$ such that $x*y = e$. Then $(G,*)$ is a group.

The element $e$ is called a **right identity**, and the element $y$ associated to $x$ is called a **right inverse** of $x$. In order to prove the theorem, we have to show that $G$ satisfies all the axioms for a group, and since we have assumed that $*$ is a binary operation on $G$ that is associative, we have only to verify that $e$ is, in fact, also a **left identity**, that is, $e*x = x$ for all $x \in G$, and that a right inverse $y$ of $x$ is also, in fact, a **left inverse** of $x$, that is, $y*x = e$.

*PROOF OF THE THEOREM.* First we show that $e*x = x$ for all $x \in G$. Let us do the proof backwards by trying to find some equation that we know would yield $e*x = x$. Let $x'$ denote a right inverse of $x$. Surely it would be enough to have

$$(\quad)*x' = \quad, \qquad [3.1]$$

for then we could multiply both sides of a right inverse $x'$. But having [3.1] is the same thing as having

$$e*(x*x') = x*x',$$



by associativity, and this is known as having

$$e* = ,$$

by the definition of a right inverse $x'$. Certainly we know that $e*e = e$, because $x*e = x$ for any $x$.

We have proved $e*x = x$ because each successive equation in our proof implied the one before it, so that when we finally arrived at a true equation,

Thm 3.6

$x*y = x*z \Rightarrow y = z$

mult by $x^{-1}$ on left

$x^{-1}*x*y = x^{-1}*x*z$

$e*y = e*z$

$y = z$

$y*x = z*x \Rightarrow y = z$

mult by $x^{-1}$ on right

...

12:17 AM Tue Sep 1

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra &... | Linear Algebra

work with in establishing that some system is in fact a group.

**THEOREM 3.7** Let $G$ be a set and $*$ an associative binary operation on $G$. Assume that there is an element $e \in G$ such that $x*e = x$ for all $x \in G$, and assume that for any $x \in G$ there exists an element $y$ in $G$ such that $x*y = e$. Then $(G, *)$ is a group.

The element $e$ is called a **right identity**, and the element $y$ associated to $x$ is called a **right inverse** of $x$. In order to prove the theorem we have to show that $G$ satisfies all the axioms for a group, and since we have assumed that $*$ is a binary operation on $G$ and $*$ is associative, we have only to verify that $e$ is, in fact, also a **left identity**, that is, $e*x = x$ for all $x \in G$; and that a right inverse $y$ of $x$ is also, in fact, a **left inverse** of $x$, that is, $y*x = e$.

*PROOF OF THE THEOREM.* First we show that $e*x = x$ for all $x \in G$. Let us do the proof backwards by trying to obtain some equations that we know would yield $e*x = x$. Let $x'$ denote a right inverse of $x$. Certainly it would be enough to have

$$(x*x')*x = x*x', \qquad [3.1]$$

for then we could multiply both sides by a right inverse of $x'$. But having [3.1] is the same thing as having

$$e*(x*x') = x*x',$$

30 **Section 3. Fundamental Theorems about Groups**

by associativity, and this is the same thing as having

$$e*e = e,$$

by the definition of the right inverse $x'$. Certainly we know that $e*e = e$, because $x*e = x$ for any $x \in G$.

We have proved $e*x = x$, because each successive equation in our proof implied the one before it, so that when we finally arrived at a true equation, the truth implied the truth of all the previous equations. It is crucial to realize that in this situation it would not have sufficed to have each equation implying the one *after* it. In other words, if we want to prove $e*x = x$, it suffices to show that $e*x = x$ is implied by the true statement $e*e = e$, but it would not be enough to show that $e*x = x$ *implies* $e*e = e$. (A simple example: The false statement "$-1 = 1$" implies the true statement "$1 = 1$," as we see by squaring both sides; but that doesn't prove $-1 = 1$.)

Now let's finish the proof of Theorem 3.7 by showing that a right inverse $x'$ of $x$ is also a left inverse of $x$, that is, $x'*x = e$. We know that there is some $(x')'$ such that $x'*(x')' = e$, and it will suffice to show that $x = (x')'$. Now from

$x*x' = e$

Modern Algebra & Number Systems

Modern Algebra &... | Abstract_Algebra_1-5 | Linear Algebra

**Thm 3.7** If $G$ is a set of elements and $*$ is a binary operation on $G$

$\forall a,b \in G \quad a*b \in G$

that is associative

$\forall a,b,c \in G \quad (a*b)*c = a*(b*c)$

and $\exists e \in G$ s.t $x*e = x \quad \forall x \in G$

only check one side ✓

and $\forall x \in G \ \exists y \in G \quad x*y = e$

then $(G, *)$ is a group.

**Must prove**

Part I also $e*x = x \quad \forall x \in X$

Part II $\forall x \in G \ \exists y \in G$ s.t

$x*y = y*x = e$

Try to write proof & then we'll do it together!

1:02 AM Tue Sep 1

Modern Algebra & Number Systems

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

**Thm 3.7** If $G$ is a set of elements and $*$ is a binary operation on $G$

$\forall a,b \in G \quad a*b \in G$

that is associative

$\forall a,b,c \in G \quad (a*b)*c = a*(b*c)$

and $\exists e \in G$ s.t. $x*e = x \quad \forall x \in G$ (Right Identity)

and $\forall x \in G \quad \exists x_R \in G \quad x * x_R = e$ (Right Inverse)

then $(G,*)$ is a group.

**Must prove:**

Part I $\exists e \in G$ s.t. $x*e = e*x = x \quad \forall x \in G$

Part II $\forall x \in G \quad \exists y \in G$ s.t. $x*y = y*x = e$

$x_R$ is the right inverse

Be careful with cancelling

$e * e = e$

$e * (x * x^{-1}) = (x * x^{-1})$

$(e * x) * x^{-1} = x * x^{-1}$

$(e * x) * x^{-1}) * (x^{-1})^{-1} = (x * x^{-1}) * (x^{-1})^{-1}$

$e * x * e = x * e$

$e * x = x * e$

---

Modern Algebra & Number Systems

Modern Algebra &... | Abstract_Algebra_1-5 | Linear Algebra

Cannot use $(x^{-1})^{-1} = x$

Cannot use cancellation

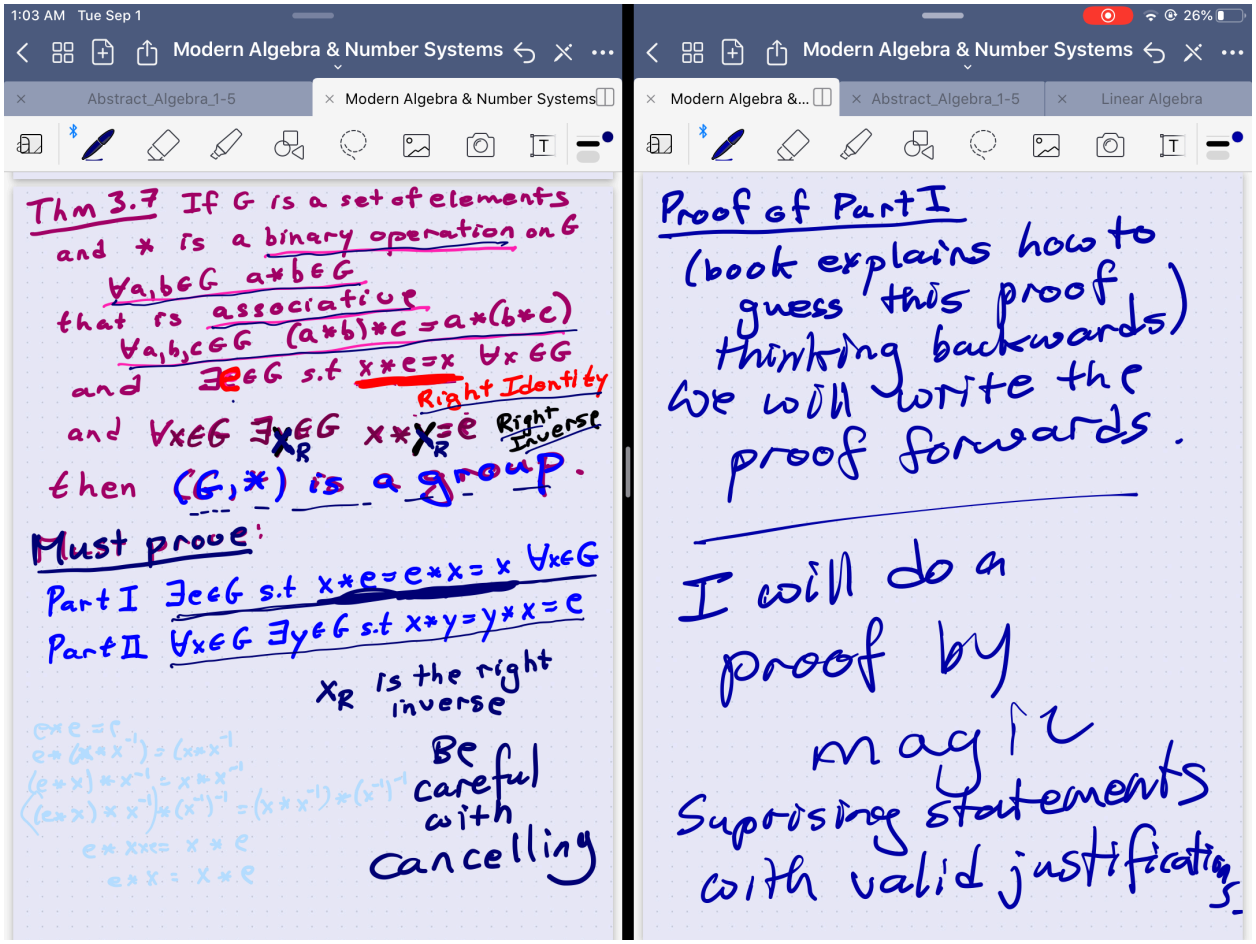
$x*a = x*b$

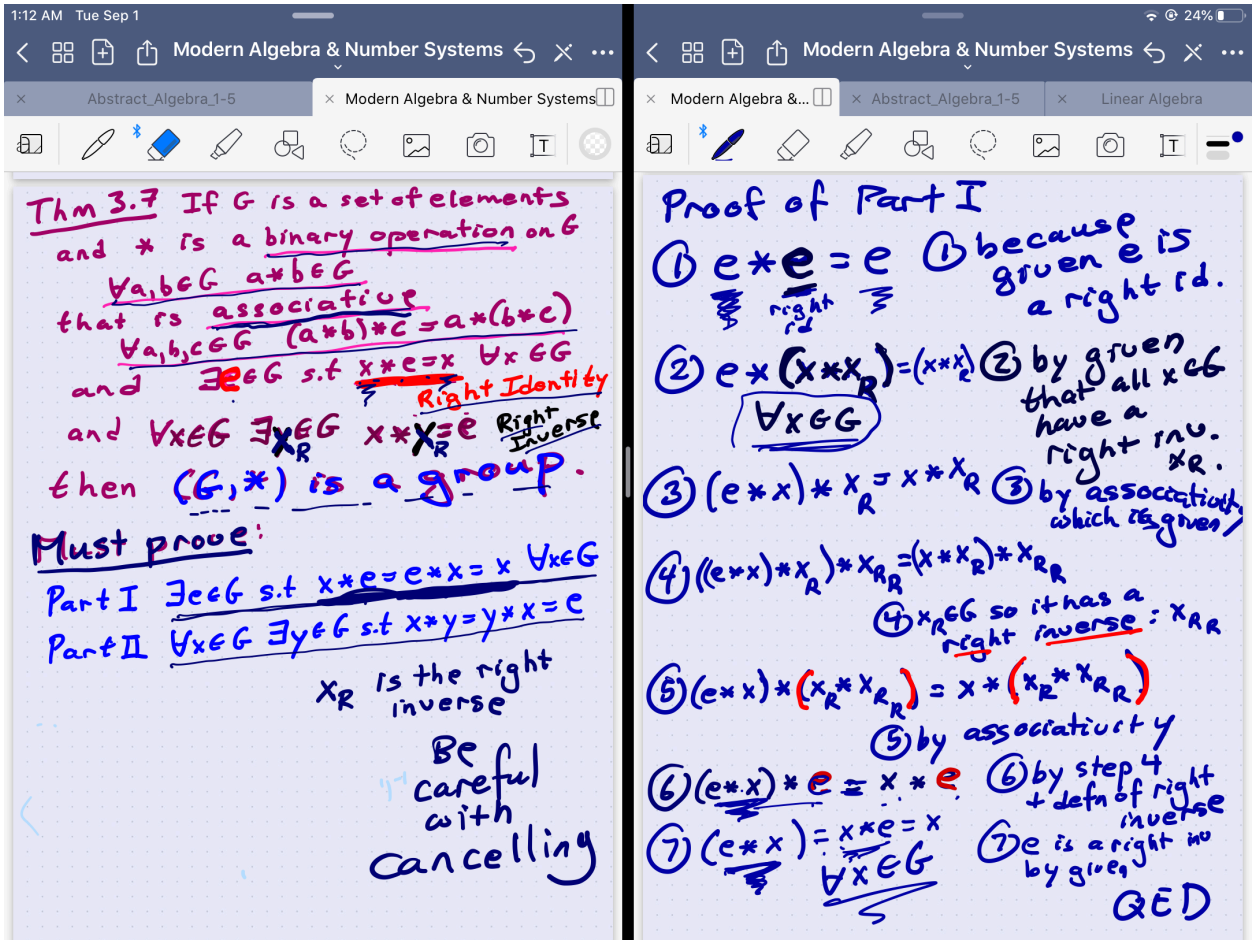
$\Downarrow$

$a = b$

This would need a left inverse

Can


1:03 AM Tue Sep 1
Modern Algebra & Number Systems
Abstract_Algebra_1-5
Modern Algebra & Number Systems
Thm 3.7 If G is a set of elements and * is a binary operation on G
∀a,b∈G a*b∈G
that is associative
∀a,b,c∈G (a*b)*c=a*(b*c)
and ∃e∈G s.t x*e=x ∀x∈G
Right Identity
and ∀x∈G ∃x_R∈G x*x_R=e
Right Inverse
then (G,*) is a group.
Must prove:
Part I ∃e∈G s.t x*e=e*x=x ∀x∈G
Part II ∀x∈G ∃y∈G s.t x*y=y*x=e
x_R is the right inverse
Be careful with cancelling
Modern Algebra &...
Abstract_Algebra_1-5
Linear Algebra
Proof of Part I
(book explains how to guess this proof thinking backwards)
We will write the proof forwards.
I will do a proof by magic
Supposing statements with valid justifications




**HW7: Fill in the justifications in the following 3 proofs for Thm 3.7 Part II and determine which 1 or 2 of the following 3 proofs is correct. Be careful only to use right inverses. You may use Part I to justify a step in Part II.**

**Thm 3.7** If $G$ is a set of elements and $*$ is a binary operation on $G$ that is associative and $\exists e \in G$ s.t. $x*e=x \ \forall x \in G$ and $\forall x \in G \ \exists x_R \in G$ s.t. $x*x_R=e$, then $(G,*)$ is a group.

(Right Identity; Right Inverse)

**Must prove:**

Part I $\exists e \in G$ s.t. $x*e=e*x=x \ \forall x \in G$

Part II $\forall x \in G \ \exists y \in G$ s.t. $x*y=y*x=e$

$x_R$ is the right inverse

Be careful with cancelling

Is this a proof of Part II?

① $x * x_R = e$ ①

② $(x * x_R) * x = e * x$ ②

③ $x_R * (x * x_R) * x = x_R * (e * x)$ ③

④ $(x_R * x) * (x_R * x) = x_R * x$ ④

⑤ $e * (x_R * x) = e$ ⑤

⑥ $x_R * x = e$ ⑥

Fill in justifications and determine if any steps are wrong.

QED

Is this a proof of Part II?

(1) $x * x_R = e$ (1)

(2) $(x * x_R) * x = e * x$ (2)

(3) $x_R * (x * x_R) * x = x_R * (e * x)$ (3)

(4) $(x_R * x) * (x_R * x) = x_R * x$ (4)

(5) Let $b = x_R * x$ (5)

then $b * b = b$

(6) $(b * b) * b_R = b * b_R$ (6)

(7) $b * (b * b_R) = b * b_R$ (7)

(8) $b * e = e$ (8)

(9) $b = e$ (9)

(10) $x_R * x = e$ (10)

QED

Is this a proof of Part II?

(1) Let $a = x_R * x$ (1)

Then $a \in G$

(2) $a * a = (x_R * x) * (x_R * x)$ (2)

(3) $a * a = x_R * (x * x_R) * x$ (3)

(4) $a * a = x_R * e * x$ (4)

(5) $a * a = x_R * x$ (5)

(6) $a * a = a$ (6)

(7) $a * a * a_R = a * a_R$ (7)

(8) $a * e = e$ (8)

(9) $a = e$ (9)

(10) $x_R * x = e$ (10)

QED

There are 7 homework problems listed above and discussed with hints in the videos.

**Start a new homework googledoc with the same template as before and name it**
**MAT314F20ex2-lastname-firstname**
**or**
**MAT615F20ex2-lastname-firstname**
**for all lessons leading to exam 2.**

***Warning: homework must be done following the methods taught in the videos. If not done this way, the feedback will simply be "watch the videos". Everyone will have exactly one opportunity to receive feedback and resubmit work. Don't waste that opportunity by not watching the videos.***

**.**
**Since there is only one correct answer to the problems in Lesson 7, I share the perfect solutions by one student here. You can use these to check your work after you are done doing the homework. Hopefully this will help students catch up quickly rather than waiting 24 hours for feedback. I will still be grading hw that has more than one correct answer in future lessons..**

MAT 615 HW 7

Jessica Chase
9/15/20

1. Justify textbook second proof of Thm 3.2 (p.26)

| | |
|---|---|
| (1) Assume on the contrary there are 2 inverses $y_1 \neq y_2$ | (1) Indirect Hypothesis |
| (2) $x * y_1 = y_1 * x = e$ | (2) $y_1$ is an inverse by step 1, def of inverse |
| (3) $x * y_2 = y_2 * x = e$ | (3) $y_2$ is an inverse by step 1, Def of inverse |
| (4) $(y_1 * x) * y_2 = e * y_2$ | (4) $* y_2$ right sides of step 2 |
| (5) $(y_1 * x) * y_2 = y_2$ | (5) Def of identity |
| (6) $y_1 * (x * y_2) = y_2$ | (6) associativity |
| (7) $y_1 * e = y_2$ | (7) By step 3 |
| (8) $y_1 = y_2$ | (8) Def of identity |

⊗ There are not 2 inverses, there is only 1 □

☞ $\otimes$ $y_1 \neq y_2$

2. Justify textbook proof Thm 3.3 (p.27)
If $(G,*)$ is a group then for any $x \in G$, $(x^{-1})^{-1} = x$

| | |
|---|---|
| (1) $x * x^{-1} = x^{-1} * x = e$ | (1) Given $(G,*)$ is a group, Def of inverse |
| (2) $(x^{-1})^{-1} = x$ | (2) By step 1 x satisfies the def of inverse for $x^{-1}$ |

□

3. Justify textbook 2nd proof Thm 3.3 (p.27)
If $(G,*)$ is a group then for any $x \in G$, $(x^{-1})^{-1} = x$

| | |
|---|---|
| (1) $x * x^{-1} = x^{-1} * x = e$ | (1) Given $(G,*)$ is a group Def of inverse |
| (2) $(x^{-1})^{-1} * (x^{-1} * x) = (x^{-1})^{-1} * e$ | (2) $* x^{-1}$ on left both sides step 1 |
| (3) $((x^{-1})^{-1} * x^{-1}) * x = (x^{-1})^{-1} * e$ | (3) associativity |
| (4) $((x^{-1})^{-1} * x^{-1}) * x = (x^{-1})^{-1}$ | (4) Def of identity |
| (5) $e * x = (x^{-1})^{-1}$ | (5) Def of inverse |
| (6) $x = (x^{-1})^{-1}$ | (6) Def of identity |

□



MAT 615 HW 7

4. Prove Thm 3.4: If $(G,*)$ is a group and $x, y \in G$, then $(x*y)^{-1} = y^{-1} * x^{-1}$

Show $(x*y)*(y^{-1}*x^{-1}) = e$

| | |
|---|---|
| (1) $(x*y)*(y^{-1}*x^{-1}) = x*(y*(y^{-1}*x^{-1}))$ | (1) associativity Given $(G,*)$ group |
| (2) $= x*((y*y^{-1})*x^{-1})$ | (2) associativity |
| (3) $= x*(e*x^{-1})$ | (3) Def of inverse |
| (4) $= x*x^{-1}$ | (4) Def of identity |
| (5) $= e$ | (5) Def of inverse |

Perfect!

Show other direction

| | |
|---|---|
| (6) $(y^{-1}*x^{-1})*(x*y) = y^{-1}*(x*(x*y))$ | (6) associativity |
| (7) $= y^{-1}*((x^{-1}*x)*y)$ | (7) associativity |
| (8) $= y^{-1}*(e*y)$ | (8) Def of inverse |
| (9) $= y^{-1}*y$ | (9) Def of identity |
| (10) $= e$ | (10) Def of inverse |

$(y^{-1}*x^{-1})$ satisfies conditions for being the inverse of $(x*y)$. By Thm 3.2 the inverses are unique therefore $(x*y)^{-1} = y^{-1}*x^{-1}$ □

6. Justify both proof of Thm 3.5
Let $(G,*)$ be a group and let $x,y \in G$. Suppose that either $x*y=e$ or $y*x=e$ then $y=x^{-1}$

| | |
|---|---|
| (1) $x*y=e$ | (1) Given |
| (2) $x^{-1}*(x*y)=x^{-1}*e$ | (2) $x^{-1}*$ left both sides, $x^{-1} \in G$, given $(G,*)$ group |
| (3) $(x^{-1}*x)*y=x^{-1}*e$ | (3) associativity, given $(G,*)$ grp |
| (4) $e*y=x^{-1}*e$ | (4) Def of inverse |



MAT 615 HW 7

Jessica Chue

continued

| | |
|---|---|
| 6. (5) $y=x^{-1}$ | (5) Def of identity |
| Other supposition | |
| (6) $y*x=e$ | (6) Given |
| (7) $(y*x)*x^{-1}=e*x^{-1}$ | (7) $*x^{-1}$ right both sides, $x^{-1} \in G$, given $(G,*)$ group |
| (8) $y*(x*x^{-1})=e*x^{-1}$ | (8) associativity, given $(G,*)$ grp |
| (9) $y*e=e*x^{-1}$ | (9) Def of inverse |
| (10) $y=x^{-1}$ | (10) Def of identity |

Excellent

□

7. Part II Thm 3.7

If G is a set of elements and $*$ is a binary operation on G, $\forall a,b \in G$ $a*b \in G$ that is associative $\forall a,b,c \in G$, $a*(b*c) = (a*b)*c$ and $\exists e \in G$ such that $x*e_R = x$ (right identity) $\forall x \in G$. and $\exists \forall x \in G \; \exists x_R \in G$, $x * x_R = e$ (right inverse) then $(G, *)$ is a group

(a) Is this a proof of Part II? (Show $\forall x \in G$, $\exists y \in G$ st $xy = e$)

| | |
|---|---|
| (1) $x * x_R = e$ | (1) Given |
| (2) $(x * x_R) * x = e * x$ | (2) $*x$ on right both sides |
| (3) $x_R * (x * x_R) * x = x_R * (e * x)$ | (3) $x_R *$ on left both sides |
| (4) $(x_R * x) * (x_R * x) = x_R * x$ | (4) given $*$ associative, Part I |
| (5) $e * (x_R * x) = e$ | (5) def of inverse |
| (6) $x_R * x = e$ | (6) Pf I left identity |

No, Step 5 is not justified ($x_R * x = e$) because we are only given a right inverse not a left inverse.

MAT 615 HW7 Jenica Cave

(b) Is this a proof of part II?

| | |
|---|---|
| (1) $x * x_R = e$ | (1) Given |
| (2) $(x * x_R) * x = e * x$ | (2) $*x$ on right both sides |
| (3) $x_R * (x * x_R) * x = x_R * (e * x)$ | (3) $x_R *$ on left both sides |
| (4) $(x_R * x) * (x_R * x) = x_R * x$ | (4) associativity, Part I |
| (5) Let $b = x_R * x$. Then $b*b = b$ | (5) By step 4 |
| (6) $(b*b) * b_R = b * b_R$ | (6) $* b_R$ right both sides |
| (7) $b * (b * b_R) = b * b_R$ | (7) associativity |
| (8) $b * e = e$ | (8) Def of right inverse |
| (9) $b = e$ | (9) Def right inv & right identity |
| (10) $x_R * x = e$ | (10) by Step 5 |

Yes, this is a valid proof

(c) Is this a proof of Part II?

| | |
|---|---|
| (1) Let $a = x_R * x$. Then $a \in G$ | (1) Given $*$ binary operation |
| (2) $a*a = (x_R * x) * (x_R * x)$ | (2) By step 1 |
| (3) $a*a = x_R * (x * x_R) * x$ | (3) given $*$ is associative |
| (4) $a*a = x_R * e * x$ | (4) Def of right inverse |
| (5) $a*a = x_R * x$ | (5) Part I left identity |
| (6) $a*a = a$ | (6) By step 1 |
| (7) $a*a*a_R = a*a_R$ | (7) $* a_R$ on right both sides |
| (8) $a*e = e$ | (8) Def of right inverse |
| (9) $a = e$ | (9) Def of right identity |
| (10) $x_R * x = e$ | (10) By step 1 |

Yes, this is a valid proof.