

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 $(G, \cdot)$ 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 $x \cdot e = e \cdot x = x$ for all x in G and $x \cdot e_1 = e_1 \cdot x = x$ 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)

$$e_1 \cdot e = e \cdot e_1 = e_1.$$

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

$$e \cdot e_1 = e_1 \cdot e = e.$$

Thus we have $e_1 = e \cdot e_1 = e$, and the proof is complete. $\square$

THEOREM 3.2 (Uniqueness of inverses) If $(G, \cdot)$ 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 $x \cdot y_1 = y_1 \cdot x = e$ and $x \cdot y_2 = y_2 \cdot x = e$, 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

$$\forall x \in G \quad \exists y \in G \text{ s.t. } x * y = y * x = e.$$

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 $(G, \cdot)$ 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 $x \cdot e = e \cdot x = x$ for all x in G and $x \cdot e_1 = e_1 \cdot x = x$ 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)

$$e_1 \cdot e = e \cdot e_1 = e_1.$$

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

$$e \cdot e_1 = e_1 \cdot e = e.$$

Thus we have $e_1 = e \cdot e_1 = e$, and the proof is complete. $\square$

THEOREM 3.2 (Uniqueness of inverses) If $(G, \cdot)$ 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 $x \cdot y_1 = y_1 \cdot x = e$ and $x \cdot y_2 = y_2 \cdot x = e$, 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

$$\forall x \in G \quad \exists y \in G \text{ s.t. } x * y = y * x = e.$$

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

11:15 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:

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

that is associative:

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

has an identity element:

$$\exists e \in G \text{ s.t. } \forall x \in G \quad e * x = x * e = x$$

and inverses:

$$\forall x \in G \quad \exists y \in G \text{ s.t. } x * y = y * x = e$$

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. $\square$

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

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

Examples All had unique Identity Elements!

$(\mathbb{Z}_p, + \text{ mod } p)$
 0 was the identity
 $0 + a = a + 0 = a$

$(\mathbb{Q}_+, \cdot)$
 1 was the identity
 $1 \cdot \frac{p}{2} = \frac{p}{2} = 1 = \frac{p}{2} \quad \forall \frac{p}{2} \in \mathbb{Q}$

$(GL(2, \mathbb{R}), \cdot)$
 $Id = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

11:30 PM Mon Aug 31

Abstract_Algebra_1-5

Abstract_Algebra_1-5

SECTION 3

Lesson 7

FUNDAMENTAL THEOREMS ABOUT GROUPS

Defn A group $(G, *)$ is a set G with a binary operation:

- $\forall a, b \in G, a * b \in G$
- 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 $e = e * e_1 = e$, and the proof is complete. $\square$

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 $e_1 \in G$

② $x * e = e * x = x \quad \forall x \in G$

③ $x * e_1 = e_1 * x = x \quad \forall x \in G$

④ $e_1 * e = e * e_1 = e_1$

⑤ $e * e_1 = e_1 * e = e$

⑥ $e_1 = e * e_1 = e$

⑦ They are the same. Not two!

⑧ by step 1 e is an identity element and defn of identity

⑨ by step 1 e_1 is an identity element and defn of identity

⑩ Taking $x = e_1$ in step 2

⑪ Taking $x = e$ in step 3

⑫ by steps 4 + 5 and $a = b$ and $b = c \Rightarrow a = c$

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. $\square$

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*

25

26 Section 3. Fundamental Theorems about Groups

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

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

$$e * y_1 = e * y_2,$$

$$y_1 = y_2$$

as desired. $\square$

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 :

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

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

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

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

11:47 PM Mon Aug 31

Abstract_Algebra_1-5

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

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

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*

25

26 Section 3. Fundamental Theorems about Groups

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 . 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

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

$$e * y_1 = e * y_2$$

$$y_1 = y_2$$

as desired. $\square$

The proof is finished, but we are now in a position to gain insight into why different inverses of an element x must be equal. We can see this by looking at the equation $x * y_1 = y_1 * x = e$ and 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 remove the x from the left-hand side, you need y_2 on the right, the only way to do this is already on the left, and we cannot get y_2 on the right by multiplying both sides by

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

$$= y_2$$

Now if only we could get rid of y_1 on the left-hand side, we'd be done; but now we have a problem: we can't start with $y_1 * x = e$, so we remove the left side by using associativity, so as to bring $x * y_2$ into play:

Modern Algebra & Number Systems

Modern Algebra &... x Abstract_Algebra_1-5 x 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

⑥ $(y_1 * x) * y_1 = (y_1 * x) * y_2$ ⑥ by associativity

⑦ $e * y_1 = e * y_2$ ⑦ by step 2

⑧ $y_1 = y_2$ ⑧ by defn of e identity

Only one inverse. QED

HW1 is in here:

11:51 PM Mon Aug 31

Abstract_Algebra_1-5

Abstract_Algebra_1-5 Modern Algebra &... Linear Algebra

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 :

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

By using associativity, we get from this

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

$$e * y_2 = e * y_2.$$

$$y_1 = y_2.$$

as desired. $\square$

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 :

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

$$= y_2.$$

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:

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

$$y_1 * e = y_2,$$

$$y_1 = y_2,$$

and we are done. $\square$

We emphasize the significance of what we have just proved twice: The group axioms simply assert that for any x , there must exist an inverse; our theorem says that once you know you've got a group, any x has precisely one inverse.

Section 3. Fundamental Theorems about Groups 27

Example Let $(G, *)$ be $GL(2, \mathbb{R})$. Then by applying our general result in this specific case, we conclude that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an invertible matrix, then there is only one matrix $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ such that

Modern Algebra & Number Systems

Modern Algebra &... Abstract_Algebra_1-5 Linear Algebra

HW1

Write up a second proof of Thm 3.2 following the book

← It starts like before with y_1 and y_2 are inverses. Same ① ② & ③ as we had which includes $y_1 * x = e$ then follow second proof.

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

12:05 AM Tue Sep 1

Abstract_Algebra_1-5

Section 3. Fundamental Theorems about Groups 27

Example Let $(G, *)$ be $(\mathbb{Z}/2\mathbb{Z}, \mathbb{R})$. Then by applying our general result in this specific case, we conclude that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an invertible matrix, then there is only one matrix $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

This fact can of course be established directly, by working with systems of linear equations in two variables. By one is struck by the economy and elegance of the "cleanness" of the proof we have obtained by viewing the collection of all invertible 2×2 matrices as a group.

Henceforth we will usually denote the unique inverse of x by x^{-1} . When we are dealing with a abelian group and referring to the group operation as addition, however, we will sometimes denote the inverse of x by $-x$. For example, in $(\mathbb{Z}/2\mathbb{Z}, \mathbb{R})$ we write

$$\begin{pmatrix} 4 & 5 \\ 1 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix}$$

and in $(\mathbb{Z}/2\mathbb{Z}, \mathbb{R})$ we write $-4 = 4$.

The next result will enable us to conclude that no two distinct elements of a group G can have the same inverse.

THEOREM 3.3 If $(G, *)$ is a group, then for any $x \in G$ we have $(x^{-1})^{-1} = x$.

PROOF. Since x^{-1} is the inverse of x , we know that $x^{-1} * x = x * x^{-1} = e$. By these equations, x satisfies the definition of $(x^{-1})^{-1}$, so $x = (x^{-1})^{-1}$ by the uniqueness of inverses. $\square$

That was slick, but let's do it again in a slightly different way. We know that $x^{-1} * x = e$. We want to get from this to an equation with x on one side and $(x^{-1})^{-1}$ on the other. We need to get rid of the x^{-1} on the left side, so let's multiply both sides by $(x^{-1})^{-1}$:

$$\begin{aligned} (x^{-1})^{-1} * (x^{-1} * x) &= (x^{-1})^{-1} * e \\ ((x^{-1})^{-1} * x^{-1}) * x &= (x^{-1})^{-1} \quad (\text{using associativity on the left}) \\ e * x &= (x^{-1})^{-1} \\ x &= (x^{-1})^{-1}. \quad \square \end{aligned}$$

Modern Algebra & Number Systems

HW2:

Thm 3.3 If $(G, *)$ is a group then $\forall x \in G$ $(x^{-1})^{-1} = x$.

Write up this proof

HW3

Write up this proof

Two column format

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

12:05 AM Tue Sep 1

Abstract_Algebra_1-5

Abstract_Algebra_1-5 Modern Algebra &... Linear Algebra

Example Let $G = (\mathbb{Z}, +)$. Then for this example the theorem says that $-(-n) = n$ for any integer n .

Now suppose x, y are elements of a group $(G, \cdot)$ and $x^{-1} = y^{-1}$. Then by taking inverses on both sides we get $(x^{-1})^{-1} = (y^{-1})^{-1}$, so, by the theorem, $x = y$. Thus, as promised, if two elements have the same inverse then they must in fact be the same element. It is possible to prove this without reference to the preceding theorem; see Exercise 3.8(b).

Next we examine the inverse of a product.

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

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

PROOF.

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot (y^{-1} \cdot x^{-1}))$$

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

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

It is worth emphasizing the reversal of order in the above result. In general, it is not true that $(x \cdot y)^{-1}$ is $x^{-1} \cdot y^{-1}$. This does, of course, hold true in *abelian* groups, for then $x^{-1} \cdot y^{-1}$ is the same thing as $y^{-1} \cdot x^{-1}$. In fact, the equation $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$ 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 $x \cdot y \cdot (y^{-1} \cdot x^{-1}) = e$ and $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = e$ 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 $(G, \cdot)$ be a group and let $x, y \in G$. Suppose that either $x \cdot y = e$ or $y \cdot x = e$. Then y is x^{-1} .

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

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

Modern Algebra & Number Systems

Modern Algebra &... Abstract_Algebra_1-5 Linear Algebra

HW4

Prove Thm 3.4

$$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$$

↑ ↑
reverses
order

Write up the proof in 2 columns

HW5 Why do we need to switch the orders Exercise 3.9.

Section 3. Fundamental Theorems about Groups 29

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 $(G, \cdot)$ is a group and $x, y \in G$, then

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

PROOF.

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot (y^{-1} \cdot x^{-1}))$$

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

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

It is worth emphasizing the reversal of order in the above result. In general, it is not true that $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$. This does, of course, hold true in *commutative* groups, but then $x^{-1} \cdot y^{-1}$ is the same thing as $y^{-1} \cdot x^{-1}$. In fact, the equation $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$ 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 $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = e$ and $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = e$ 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 $(G, \cdot)$ be a group and let $x, y \in G$. Suppose that either $x \cdot y = e$ or $y \cdot x = e$. Then y is x^{-1} .

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

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

Section 3. Fundamental Theorems about Groups 29

Thus

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

$$e \cdot y = x^{-1} \cdot e,$$

$$y = x^{-1} \cdot e.$$

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

The same solving of an equation proves the more general

Modern Algebra & Number Systems

Modern Algebra &... Abstract_Algebra_1-5 Linear Algebra

Thm 3.5:

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

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 the **identity**. 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 , it 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 the right inverse of x ; clearly it would be enough to have

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

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 associating, and this is the same thing as having

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

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

...

work with an ~~equation~~ ~~that~~ ~~some~~ ~~system~~ is ~~in~~ ~~fact~~ ~~a~~ ~~group~~.

THEOREM 3.7 Let G be a set and $\cdot$ an associative binary operation on G . Assume that there is an element $e \in G$ such that $x \cdot e = x$ for all $x \in G$, and assume that for any $x \in G$ there exists an element $y \in G$ such that $x \cdot y = e$. Then $(G, \cdot)$ 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 $\cdot$ is a binary operation on G and $\cdot$ is associative, we have only to verify that e is, in fact, also a **left identity**, that is, $e \cdot x = x$ for all $x \in G$; and that a right inverse y of x is also, in fact, a **left inverse** of x , that is, $y \cdot x = e$.

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

$$(e \cdot x) \cdot x' = x \cdot x' \quad (3.1)$$

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

$$e \cdot (x \cdot x') = x \cdot x',$$

30 Section 3. Fundamental Theorems about Groups

by associativity, and this is the same thing as having

$$e \cdot e = e,$$

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

We have proved $e \cdot x = x$, 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 $e \cdot x = x$, it suffices to show that $e \cdot x = x$ is implied by the true statement $e \cdot e = e$, but it would not be enough to show that $e \cdot x = x$ implies $e \cdot e = e$. (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, $x' \cdot x = e$. We know that there is some $(x')'$ such that $x' \cdot (x')' = e$, and it will suffice to show that $x = (x')'$. Now from

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

Must prove

Part I also $e \cdot x = x \quad \forall x \in G$

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

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



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 $\exists e \in G$ s.t. $x * e = x \ \forall x \in G$ Right Identity
 and $\forall x \in G \ \exists x_R \in G \ x * x_R = e$ Right Inverse
 then $(G, *)$ is a group.

Must prove:

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

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

x_R is the right inverse

$$\begin{aligned} e * e &= e \\ e * (x * x^{-1}) &= (x * x^{-1}) \\ (e * x) * x^{-1} &= x * x^{-1} \\ (e * x) * x^{-1} * (x^{-1})^{-1} &= (x * x^{-1}) * (x^{-1})^{-1} \\ e * x x^{-1} &= x * e \\ e * x &= x * e \end{aligned}$$

Be careful with cancelling

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

Cannot use
 cancellation

$x * a = x * b$
 $\Downarrow$ This would need a left inverse
 $a = b$

Can

1:03 AM Tue Sep 1

Modern Algebra & Number Systems

Abstract_Algebra_1-5

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

$$\begin{aligned} e * e &= e \\ e * (x * x^{-1}) &= (x * x^{-1}) \\ (e * x) * x^{-1} &= x * x^{-1} \\ (e * x) * x^{-1} * (x^{-1})^{-1} &= (x * x^{-1}) * (x^{-1})^{-1} \\ e * x x^{-1} &= x * e \\ e * x &= x * e \end{aligned}$$

Be careful with cancelling

Modern Algebra & Number Systems

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 justification.

1:12 AM Tue Sep 1

Modern Algebra & Number Systems

Abstract_Algebra_1-5

Thm 3.7 If G is a set of elements and $*$ is a binary operation on G that is associative $\forall a, b \in G, a * b \in G$ 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.

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

Modern Algebra & Number Systems

Abstract_Algebra_1-5

Linear Algebra

Proof of Part I

① $e * e = e$ ① because e is a right id.

② $e * (x * x_R) = (x * x_R) * e$ ② by given that all $x \in G$ have a right inv. x_R .

③ $(e * x) * x_R = x * x_R$ ③ by associativity which is given

④ $(e * x) * x_R = (x * x_R) * x_R$ ④ $x_R \in G$ so it has a right inverse: x_{RR}

⑤ $(e * x) * (x_R * x_{RR}) = x * (x_R * x_{RR})$ ⑤ by associativity

⑥ $(e * x) * e = x * e$ ⑥ by step 4 + defn of right inverse

⑦ $(e * x) = x * e = x$ ⑦ e is a right inv by given

QED

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
 $\forall a, b \in G \ a * b \in G$
 that is associative
 $\forall a, b, c \in G \ (a * b) * c = a * (b * c)$
 and $\exists e \in G$ s.t. $x * e = x \ \forall x \in G$ Right Identity
 and $\forall x \in G \ \exists x_R \in G \ x * x_R = e$ Right Inverse
 then $(G, *)$ is a group.

Must prove:

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

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?

$$\textcircled{1} \ x * x_R = e \quad \textcircled{1}$$

$$\textcircled{2} \ (x * x_R) * x = e * x \quad \textcircled{2}$$

$$\textcircled{3} \ x_R * (x * x_R) * x = x_R * (e * x) \quad \textcircled{3}$$

$$\textcircled{4} \ (x_R * x) * (x_R * x) = x_R * x \quad \textcircled{4}$$

$$\textcircled{5} \ e * (x_R * x) = e \quad \textcircled{5}$$

$$\textcircled{6} \ x_R * x = e \quad \textcircled{6}$$

Fill in justifications QED
 and determine if
 any steps are wrong.

Is this a proof of Part II?

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

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

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

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

$$(5) \quad \text{Let } b = x_R * x \quad (5)$$

$$\text{then } b * b = b$$

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

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

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

$$(9) \quad b = e \quad (9)$$

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

QED

Is this a proof of Part II?

$$\textcircled{1} \text{ Let } a = x_R * x \quad \textcircled{1}$$

Then $a \in G$

$$\textcircled{2} a * a = (x_R * x) * (x_R * x) \quad \textcircled{2}$$

$$\textcircled{3} a * a = x_R * (x * x_R) * x \quad \textcircled{3}$$

$$\textcircled{4} a * a = x_R * e * x \quad \textcircled{4}$$

$$\textcircled{5} a * a = x_R * x \quad \textcircled{5}$$

$$\textcircled{6} a * a = a \quad \textcircled{6}$$

$$\textcircled{7} a * a * a_R = a * a_R \quad \textcircled{7}$$

$$\textcircled{8} a * e = e \quad \textcircled{8}$$

$$\textcircled{9} a = e \quad \textcircled{9}$$

$$\textcircled{10} x_R * x = e \quad \textcircled{10}$$

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

Jenica Choe
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, y_2
 - (2) $x * y_1 = y_1 * x = e$
 - (3) $x * y_2 = y_2 * x = e$
 - (4) $(y_1 * x) * y_2 = e * y_2$
 - (5) $(y_1 * x) * y_2 = y_2$
 - (6) $y_1 * (x * y_2) = y_2$
 - (7) $y_1 * e = y_2$
 - (8) $y_1 = y_2$
- ⊗ There are not 2 inverses; there is only 1. $\square$
- ~~$x_1 \neq y_2$~~

(1) Indirect Hypothesis

(2) y_1 is an inverse by step 1, def of inverse

(3) y_2 is an inverse by step 1, def of inverse

(4) $* y_2$ right sides of step 2

(5) Def of identity

(6) associativity

(7) By step 3

(8) Def of identity

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

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

MAT 615 HW 7

Jenica Choe
2

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) $(x * y) * (y^{-1} * x^{-1}) = x * (y * (y^{-1} * x^{-1}))$
 - (2) $= x * (y * y^{-1}) * x^{-1}$
 - (3) $= x * e * x^{-1}$
 - (4) $= x * x^{-1}$
 - (5) $= e$

- Show other direction
- (6) $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * (x * y))$
 - (7) $= y^{-1} * ((x^{-1} * x) * y)$
 - (8) $= y^{-1} * (e * y)$
 - (9) $= y^{-1} * y$
 - (10) $= e$

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

6. Justify both parts 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 $(G, *)$ group
(4) $e * y = x^{-1} * e$	(4) Def of inverse

3

MAT 615 HW 7

Jessica Chae

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

Excellent (8) $y * (x * x^{-1}) = e * x^{-1}$ (8) associativity, given $(G, *)$ group

(9) $y * e = e * x^{-1}$ (9) Def of inverse

(10) $y = x^{-1}$ (10) Def of identity

7. Part II Thm 3.7

Let 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 $x * e = x$ (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 | $y * x = e$ |
| (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) Part 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.

MTT 615 HW7

Jenica Case

- (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.