Modern Algebra and Number Systems

MAT314/MAT615

Lesson 5

Finite Groups and the Division Algorithm

Watch the 6 videos in the Playlist 314F20-Lesson5 pausing regularly to do the classwork and checking your work by watching the solutions. As always the photos of the lesson are here and the homework is at the end.

12:20 AM Thu Aug 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

Lesson 5
More Groups
The Division Algorithm
Tables

7. Let X be a set, let S be the set of all subsets of X, and consider the binary operation of symmetric difference on S.

This is indeed a binary operation on S, and we have seen that it is associative: $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

Is there an identity element? In other words, is there $e \in S$ such that $A \triangle e = e \triangle A = A$ for all $A \in S$? Well, $A \triangle e = A$ implies that $A \cap e = \varnothing$, and it also implies that $e \subseteq A$. Thus e would have to be the null set. Let's check that $e = \varnothing$ works:

$$A \triangle \varnothing = (A \cup \varnothing) - (A \cap \varnothing) = A - \varnothing = A,$$

and

$$\varnothing \triangle A = (\varnothing \cup A) - (\varnothing \cap A) = A,$$

so $\varnothing$ is in fact an identity element.

How about inverses? An inverse B of A would have to satisfy

$$A \triangle B = \varnothing = B \triangle A.$$

This implies that $A \subseteq B$ and $B \subseteq A$, so B would have to be A; in fact $A \triangle A = \varnothing$, so A itself *is* an inverse for A.

Thus S forms a group under the operation of symmetric difference. As a matter of notation, the set of subsets of a set X is called the **power set** of X, and denoted by $P(X)$. Thus we have the group $(P(X), \triangle)$.

Finally, we consider some groups obtained from $\mathbb{Z}$.

8. *Additive group of integers modulo n.* Let n be a positive integer and consider the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. We add the elements of $\mathbb{Z}_n$ modulo n, i.e., we add them as integers and then disregard multiples of n so as to produce an answer that is one of $0, 1, 2, \ldots, n-1$. There is a lemma which we need to make this work. (A *lemma* in mathematics is a preliminary or auxiliary result, not the main result one is aiming at.)

LEMMA 2.1 (The Division Algorithm) If a and n are integers and n is positive, then there exist *unique* integers q and r such that $a = qn + r$ and $0 \leq r < n$ (q stands for quotient and r stands for remainder).

PROOF. **We prove the existence of q and r, then the uniqueness.**

Modern Algebra & Number Systems

Modern Algebra & Number Systems | Abstract_Algebra_1-5

Still studying groups but our examples today will have finitely many elements. (1)

Clock Arithmetic

elements are actions:

advance by 1 hour

advance by 2 hours

...

advance by 8 hours

...

advance by 11 hours

not advancing 0

{1, 2, 3, 4, ...8... 11, 0}

12:21 AM Thu Aug 27

Modern Algebra & Number Systems

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

$*$ is combine actions

$1 * 2$ = advance by 1 hour and advance by 2 hours → advance by 3 hours

$1 * 2 = 3$

$3 * 10 = 1$

we can make a table.

91%

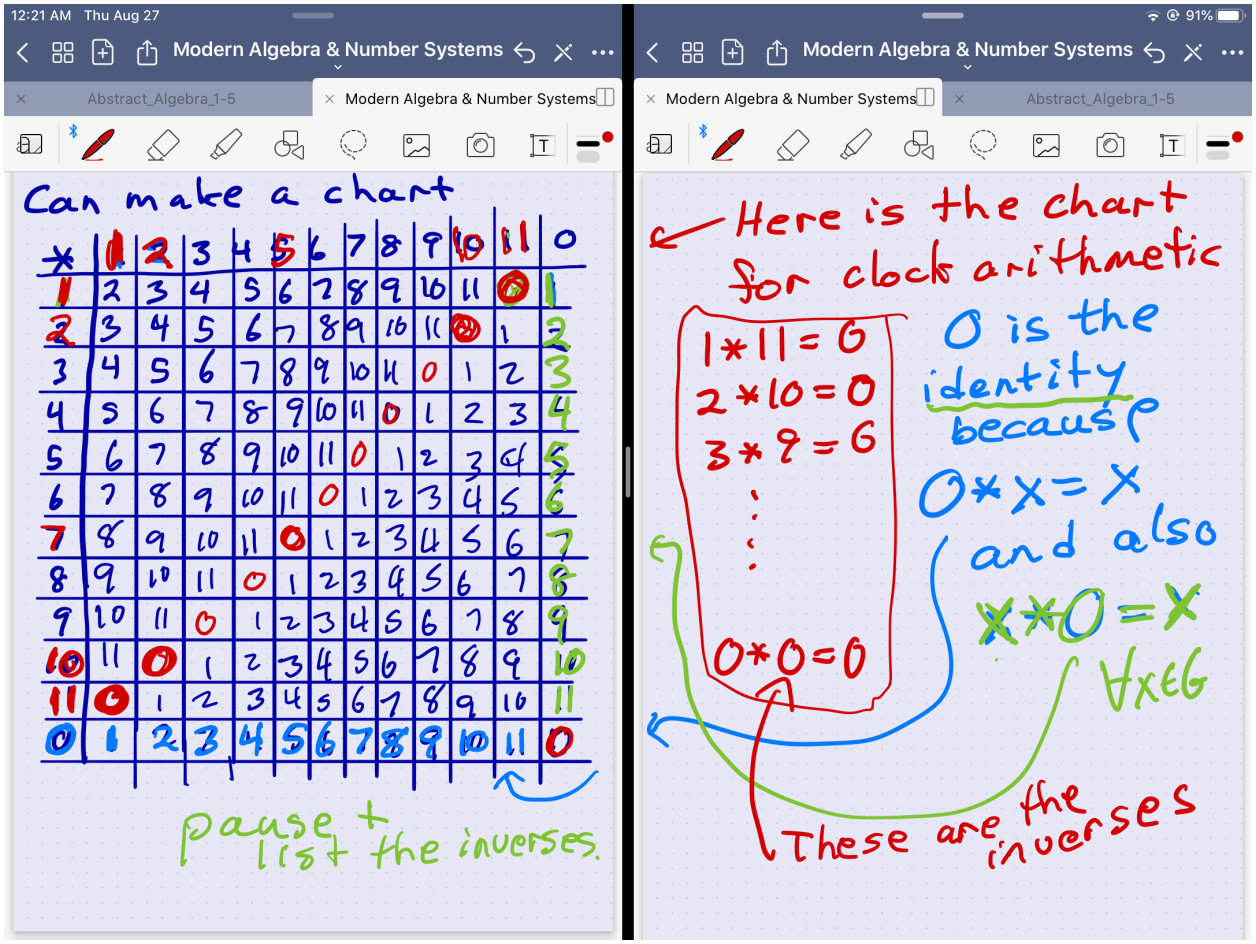
Modern Algebra & Number Systems

Modern Algebra & Number Systems | Abstract_Algebra_1-5

Can make a chart

$*$	1	2	3	4	5	6	7	8	9	10	11	0
1	2	3	4	5	6	7	8	9	10	11	0	1
2	3	4	5	6	7	8	9	10	11	0	1	2
3	4	5	6	7	8	9	10	11	0	1	2	3
4	5	6	7	8	9	10	11	0	1	2	3	4
5	6	7	8	9	10	11	0	1	2	3	4	5
6	7	8	9	10	11	0	1	2	3	4	5	6
7	8	9	10	11	0	1	2	3	4	5	6	7
8	9	10	11	0	1	2	3	4	5	6	7	8
9	10	11	0	1	2	3	4	5	6	7	8	9
10	11	0	1	2	3	4	5	6	7	8	9	10
11	0	1	2	3	4	5	6	7	8	9	10	11
0	1	2	3	4	5	6	7	8	9	10	11	0

pause + list the inverses.


12:21 AM Thu Aug 27
Modern Algebra & Number Systems
Abstract_Algebra_1-5
Modern Algebra & Number Systems
Can make a chart
Pause + list the inverses.
91%
Modern Algebra & Number Systems
Modern Algebra & Number Systems
Abstract_Algebra_1-5
Here is the chart for clock arithmetic
1*11=0
2*10=0
3*9=6
0*0=0
0 is the identity because
0*x=x
and also
x*0=x
∀x∈G
These are the inverses

12:21 AM Thu Aug 27

Modern Algebra & Number Systems

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

Can make a chart

*	1	2	3	4	5	6	7	8	9	10	11	0
1	2	3	4	5	6	7	8	9	10	11	0	1
2	3	4	5	6	7	8	9	10	11	0	1	2
3	4	5	6	7	8	9	10	11	0	1	2	3
4	5	6	7	8	9	10	11	0	1	2	3	4
5	6	7	8	9	10	11	0	1	2	3	4	5
6	7	8	9	10	11	0	1	2	3	4	5	6
7	8	9	10	11	0	1	2	3	4	5	6	7
8	9	10	11	0	1	2	3	4	5	6	7	8
9	10	11	0	1	2	3	4	5	6	7	8	9
10	11	0	1	2	3	4	5	6	7	8	9	10
11	0	1	2	3	4	5	6	7	8	9	10	11
0	1	2	3	4	5	6	7	8	9	10	11	0

pause + list the inverses.

91%

Modern Algebra & Number Systems

Modern Algebra & Number Systems | Abstract_Algebra_1-5

Inverse

$1^{-1} = 11$ $1*11=0$

$11^{-1}=1$ and $11*1=0$ ✓

$2^{-1}=10$ $2*10=0$

$10^{-1}=2$ and $10*2=0$

$3^{-1}=9 \longleftrightarrow 9^{-1}=3$ ✓

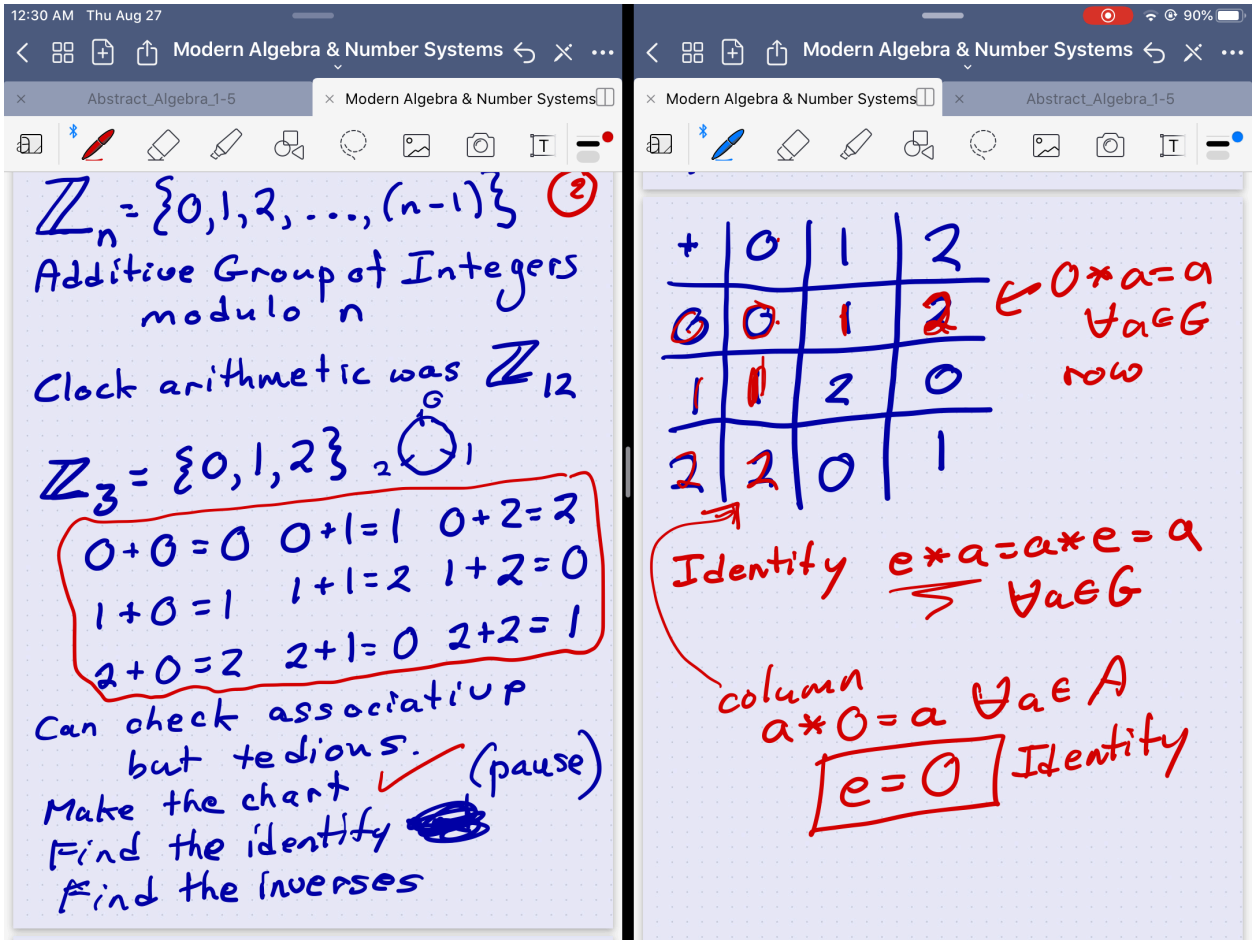
$4^{-1}=8 \longleftrightarrow 8^{-1}=4$

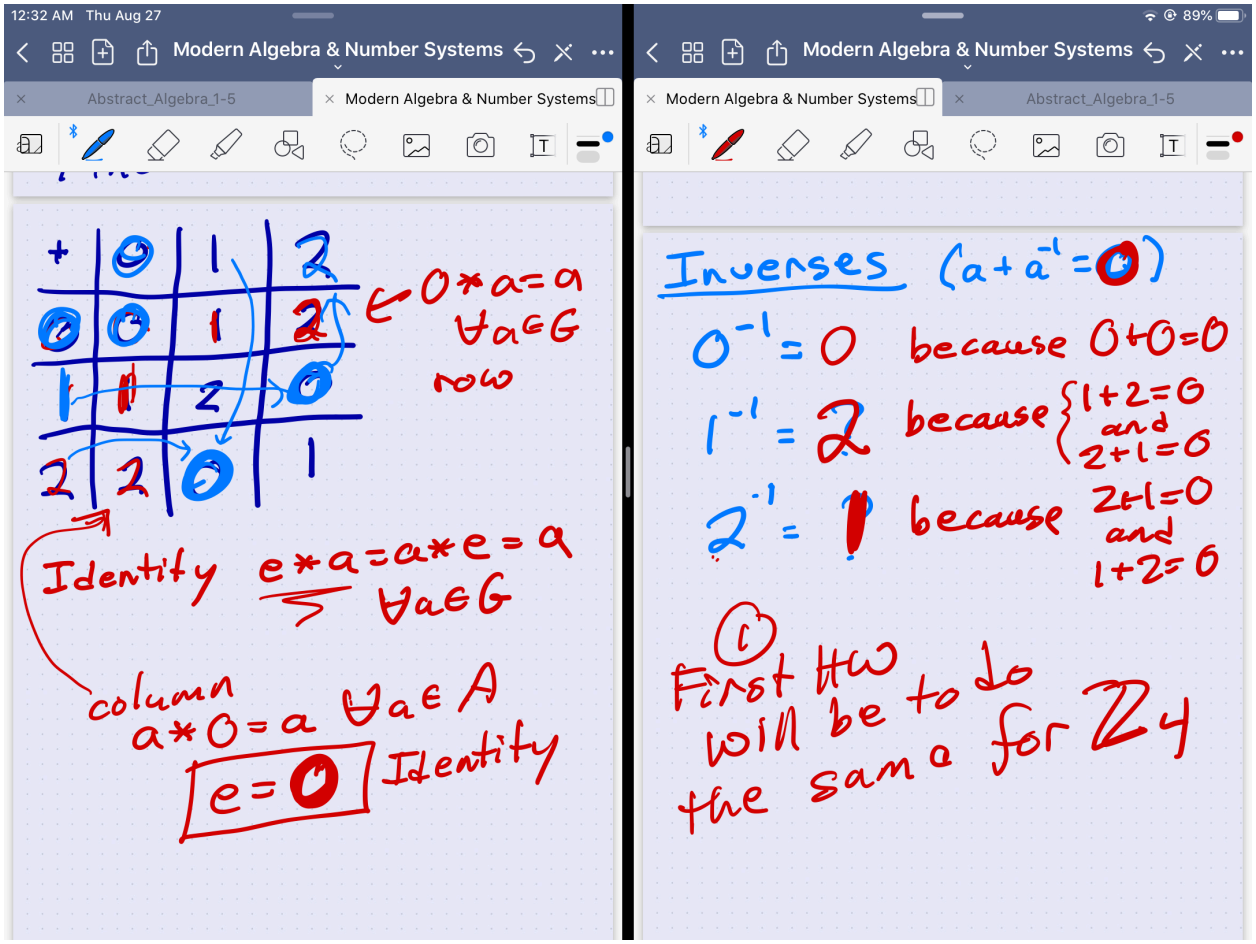
$8^{-1}=7 \longleftrightarrow 7^{-1}=5$

$6^{-1}=6$

$7^{-1}=$

Associativity because a combo of actions


12:30 AM Thu Aug 27
Modern Algebra & Number Systems
Abstract_Algebra_1-5
Modern Algebra & Number Systems
$\mathbb{Z}_n = \{0,1,2,\ldots,(n-1)\}$ (2)
Additive Group of Integers modulo n
Clock arithmetic was $\mathbb{Z}_{12}$
$\mathbb{Z}_3 = \{0,1,2\}$
0+0=0 0+1=1 0+2=2
1+0=1 1+1=2 1+2=0
2+0=2 2+1=0 2+2=1
Can check associative but tedious.
Make the chart ✓ (pause)
Find the identity
Find the inverses
Modern Algebra & Number Systems
Abstract_Algebra_1-5
90%
+ | 0 | 1 | 2
0 | 0 | 1 | 2
1 | 1 | 2 | 0
2 | 2 | 0 | 1
0*a=a ∀a∈G now
Identity e*a=a*e=a ∀a∈G
column a*0=a ∀a∈A
e=0 Identity


12:32 AM Thu Aug 27
Modern Algebra & Number Systems
Abstract_Algebra_1-5
Modern Algebra & Number Systems
89%
Modern Algebra & Number Systems
Modern Algebra & Number Systems
Abstract_Algebra_1-5
+ 0 1 2
0 0 1 2
1 1 2 0
2 2 0 1
0*a=a ∀a∈G
now
Identity e*a=a*e=a ∀a∈G
column a*0=a ∀a∈A
e=0 Identity
Inverses (a+a⁻¹=0)
0⁻¹=0 because 0+0=0
1⁻¹=2 because 1+2=0 and 2+1=0
2⁻¹=1 because 2+1=0 and 1+2=0
① First HW will be to do the same for Z4

12:44 AM Thu Aug 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

LEMMA 2.1 (The Division Algorithm) If a and n are integers and n is positive, then there exist *unique* integers q and r such that $a = qn + r$ and $0 \leq r < n$ (q stands for quotient and r stands for remainder).

PROOF. We prove the existence of q and r, then the uniqueness.

Existence: Let qn be the greatest multiple of n that is $\leq a$. If we let $r = a - qn$ then clearly $r \geq 0$ and $a = qn + r$, so all we have to check is that $r < n$. But if $r \geq n$, then

$$r - n = a - (q+1)n > 0,$$

so $(q+1)n$ is a multiple of n that is $< a$, contradicting the choice of qn as the greatest such multiple.

Uniqueness: If $q_1 n + r_1 = q_2 n + r_2$ and $0 \leq r_1 < n$, $0 \leq r_2 < n$, then

$$q_1 n - q_2 n = r_2 - r_1,$$

so $r_2 - r_1$ is a multiple of n; but $-n < r_2 - r_1 < n$, so $r_2 - r_1 = 0$, so $r_2 = r_1$. Thus $q_1 n = q_2 n$, so $q_1 = q_2$. □

We denote the unique r guaranteed by the lemma by $\bar{a}$, and call it the **remainder of a mod n.**

Observe that two integers a_1 and a_2 have the same remainder mod n iff $a_1 - a_2$ is a multiple of n. When this happens, we say that a_1 and a_2 are **congruent modulo n,** and we write $a_1 \equiv a_2 \pmod{n}$.

Examples

By the lemma we can unambiguously define a binary operation $\oplus$ on $\mathbb{Z}_n$ by setting $x \oplus y = \overline{x+y}$.

We claim that this operation turns $\mathbb{Z}_n$ into a group $(\mathbb{Z}_n, \oplus)$.

Associativity: Read in book

Lets check $\mathbb{Z}_3$

Modern Algebra & Number Systems | Abstract_Algebra_1-5

The Division Algorithm (3)

If a and $n \in \mathbb{Z}$ an $n > 0$

then $\exists!$ integers q and r

there exist unique

such that $a = qn + r$

and $0 \leq r < n$

q = quotient r = remainder

Thm If $a \in \mathbb{Z}$ $n \in \mathbb{Z}_+$ then

$\exists!$ $q, r \in \mathbb{Z}$ s.t. $a = qn + r$

and $r \in [0, n)$.

$n \overline{)a}$ q Remainder $= r$

12:49 AM Thu Aug 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

Lesson 5 More Groups The Division Algorithm Tables

7. Let X be a set, let S be the set of all subsets of X, and consider the binary operation of symmetric difference on S.

This is indeed a binary operation on S, and we have seen that it is associative: $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

Is there an identity element? In other words, is there $e \in S$ such that $A \triangle e = e \triangle A = A$ for all $A \in S$? Well, $A \triangle e = A$ implies that $A \cap e = \emptyset$, and it also implies that $e \subseteq A$. Thus e would have to be the null set. Let's check that $e = \emptyset$ works:

$$A \triangle \emptyset = (A \cup \emptyset) - (A \cap \emptyset) = A - \emptyset = A,$$

and

$$\emptyset \triangle A = (\emptyset \cup A) - (\emptyset \cap A) = A,$$

so $\emptyset$ is in fact an identity element.

How about inverses? An inverse B of A would have to satisfy

$$A \triangle B = \emptyset = B \triangle A.$$

This implies that $A \subseteq B$ and $B \subseteq A$, so B would have to be A; in fact $A \triangle A = \emptyset$, so A itself *is* an inverse for A.

Thus S forms a group under the operation of symmetric difference. As a matter of notation, the set of subsets of a set X is called the **power set** of X, and denoted by $P(X)$. Thus we have the group $(P(X), \triangle)$.

Finally, we consider some groups obtained from $\mathbb{Z}$.

8. *Additive group of integers modulo n.* Let n be a positive integer and consider the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. We add the elements of $\mathbb{Z}_n$ modulo n, i.e., we add them as integers and then disregard multiples of n so as to produce an answer that is one of $0, 1, 2, \ldots, n-1$. There is a lemma which we need to make this work. (A *lemma* in mathematics is a preliminary or auxiliary result, not the main result one is aiming at.)

LEMMA 2.1 (The Division Algorithm) If a and n are integers and n is positive, then there exist *unique* integers q and r such that $a = qn + r$ and $0 \leq r < n$ (q stands for quotient and r stands for remainder).

PROOF. We prove the existence of q and r, then the uniqueness.

Modern Algebra & Number Systems

Modern Algebra & Number Systems | Abstract_Algebra_1-5

The Division Algorithm (3)

If a and $n \in \mathbb{Z}$ $n > 0$ then $\exists!$ integers q and r (there exist unique) such that $a = qn + r$ and $0 \leq r < n$

q = quotient r = remainder

Thm If $a \in \mathbb{Z}_+$ $n \in \mathbb{Z}_+$ then $\exists!$ $q, r \in \mathbb{Z}_+$ s.t. $a = qn + r$ and $r \in [0, n)$.

$n \overline{)a}$ q Remainder $= r$

12:49 AM Thu Aug 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

LEMMA 2.1 (The Division Algorithm) If a and n are integers and n is positive, then there exist *unique* integers q and r such that $a = qn + r$ and $0 \leq r < n$ (q stands for quotient and r stands for remainder).

PROOF. We prove the existence of q and r, then the uniqueness.

Existence: Let qn be the greatest multiple of n that is $\leq a$. If we let $r = a - qn$ then clearly ~~$r \geq 0$ and $a = qn + r$~~, so all we have to check is that $r < n$. But if $r \geq n$, then

$$r - n = a - (q+1)n > 0,$$

so $(q+1)n$ is a multiple of n that is $< a$, contradicting the choice of qn as the greatest such multiple.

Uniqueness: If $q_1 n + r_1 = q_2 n + r_2$ and $0 \leq r_1 < n$, $0 \leq r_2 < n$, then

$$q_1 n - q_2 n = r_2 - r_1,$$

so $r_2 - r_1$ is a multiple of n; but $-n < r_2 - r_1 < n$, so $r_2 - r_1 = 0$, so $r_2 = r_1$. Thus $q_1 n = q_2 n$, so $q_1 = q_2$. □

We denote the unique r guaranteed by the lemma by $\bar{a}$, and call it the **remainder of a mod n.**

Observe that two integers a_1 and a_2 have the same remainder mod n iff $a_1 - a_2$ is a multiple of n. When this happens, we say that a_1 and a_2 are **congruent modulo n**, and we write $a_1 \equiv a_2 \pmod{n}$.

Examples

By the lemma we can unambiguously define a binary operation $\oplus$ on $\mathbb{Z}_n$ by setting $x \oplus y = \overline{x+y}$.

We claim that this operation turns $\mathbb{Z}_n$ into a group $(\mathbb{Z}_n, \oplus)$.

Associativity: Read in book

Lets check $\mathbb{Z}_3$

Modern Algebra & Number Systems | Abstract_Algebra_1-5

Proof Step 1 Show q and r exist.

① Let qn be the greatest multiple of n that is $\leq a$.

① $0 \cdot n \leq a$ ✓

$1 \cdot n \leq a$? if not the $q=0$ if yes continue

$2 \cdot n \leq a$? if not then $q=1$ if yes continue

⋮

Do we ever stop?

If we did not stop then $q \cdot n \leq a \ \forall q \in \mathbb{Z}^+$

but then $q \leq a \ \forall q \in \mathbb{Z}^+$

Contradicts Archimedean principle

1, 2, 3, ...

1:02 AM Thu Aug 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

Existence: Let qn be the greatest multiple of n that is $\leqslant a$. If we let $r=a-qn$ then clearly $r\geqslant 0$ and $a=qn+r$, so all we have to check is that $r<n$. But if $r\geqslant n$, then

$$r-n=a-(q+1)n\geqslant 0,$$

so $(q+1)n$ is a multiple of n that is $\leqslant a$, contradicting the choice of qn as the greatest such multiple.

Uniqueness: If $q_1n+r_1=q_2n+r_2$ and $0\leqslant r_1<n$, $0\leqslant r_2<n$, then

$$q_1n-q_2n=r_2-r_1,$$

so r_2-r_1 is a multiple of n; but $-n<r_2-r_1<n$, so $r_2-r_1=0$, so $r_2=r_1$. Thus $q_1n=q_2n$, so $q_1=q_2$. □

We denote the unique r guaranteed by the lemma by $\bar{a}$, and call it the **remainder of a mod n.**

Observe that two integers a_1 and a_2 have the same remainder mod n iff a_1-a_2 is a multiple of n. When this happens, we say that a_1 and a_2 are **congruent modulo n**, and we write $a_1\equiv a_2 \pmod n$.

Examples

By the lemma we can unambiguously define a binary operation $\oplus$ on $\mathbb{Z}_n$ by setting $x\oplus y=\overline{x+y}$.

We claim that this operation turns $\mathbb{Z}_n$ into a group $(\mathbb{Z}_n, \oplus)$.

Associativity: Read in book

Lets check $\mathbb{Z}_3$

Modern Algebra & Number Systems | Abstract_Algebra_1-5

84%

② If we let $r=a-qn$ then $r\geq 0$ and $a=qn+r$ ② by step 1 add qn to both sides

③ We claim $r<n$

③a Assume on Contrary $r\geq n$

③b add n to both sides

③b $r-n\geq 0$

$r-n=a-(q+1)n\geq 0$

$=(a-qn)-n=a-(q+1)n$ by step 2

$(q+1)n\leq a$

So $(q+1)\cdot n$ is a multiple of n that is $\leq a$.

④ choice of q in step 1

$$\begin{array}{r} 5 \\ 3\overline{)16} \\ 15 \\ \hline 1 \end{array}$$

$R = 1$

$5 \cdot 3$ is greatest multiple of $3 \leq a$

$q = 5$

$a = 16 \quad n = 3$

$$3 \cdot 5 + 1 = 16$$

$1 \in [0, 3)$

$$\begin{array}{r} 4 \\ 3\overline{)16} \\ 12 \\ \hline 4 \end{array}$$

Remainder $4 \notin [0, 3)$

not a good remainder

was not chosen big enough.

$4 \cdot 3$ is not the greatest multiple.

1:18 AM Thu Aug 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

need to make this work. (A *lemma* in mathematics is a preliminary or auxiliary result, not the main result one is aiming at.)

LEMMA 2.1 (The Division Algorithm) If a and n are integers and n is positive, then there exist *unique* integers q and r such that $a = qn + r$ and $0 \leq r < n$ (q stands for quotient and r stands for remainder).

PROOF. We prove the existence of q and r, then the uniqueness.

q remainder r

n√a

(2)

Existence: Let qn be the greatest multiple of n that is $\leq a$. If we let $r = a - qn$ then clearly $r \geq 0$ and $a = qn + r$, so all we have to check is that $r < n$. But if $r \geq n$, then (3)

(3a) (3b) $r - n = a - (q+1)n \geq 0$,

so $(q+1)n$ is a multiple of n that is $\leq a$, contradicting the choice of qn as the greatest such multiple. (4)

Uniqueness: If $q_1 n + r_1 = q_2 n + r_2$ and $0 \leq r_1 < n$, $0 \leq r_2 < n$, then

$q_1 n - q_2 n = r_2 - r_1$,

so $r_2 - r_1$ is a multiple of n; but $-n < r_2 - r_1 < n$, so $r_2 - r_1 = 0$, so $r_2 = r_1$. Thus $q_1 n = q_2 n$, so $q_1 = q_2$. □

We denote the unique r guaranteed by the lemma by $\bar{a}$, and call it the **remainder of a mod n.**

Observe that two integers a_1 and a_2 have the same remainder mod n iff $a_1 - a_2$ is a multiple of n. When this happens, we say that a_1 and a_2 are **congruent modulo n,** and we write $a_1 \equiv a_2 \pmod{n}$.

Examples

By the lemma we can unambiguously define a binary operation $\oplus$ on $\mathbb{Z}_n$ by setting $x \oplus y = \overline{x+y}$.

We claim that this operation turns $\mathbb{Z}_n$ into a group $(\mathbb{Z}_n, \oplus)$.

Associativity: Read in book

80%

Modern Algebra & Number Systems

Modern Algebra & Number Systems | Abstract_Algebra_1-5

(5)

Proof Part II Uniqueness

(1) Assume on the contrary that it is not unique

(1) Indirect hyp.

(2) Two solutions n√a

q_1 w/ remainder $r_1 \in [0, n)$

q_2 w/ remainder $r_2 \in [0, n)$

$q_1 n + r_1 = a = q_2 \cdot n + r_2$

(3) $q_1 n - q_2 n = r_2 - r_1$

(3) subtract r_1 from both sides and subtract $q_2 n$ from both side.

(4) So $r_2 - r_1$ is a multiple of n

(3) $r_2 - r_1 = n(q_1 - q_2)$ by factoring.

1:20 AM Thu Aug 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

need to make this work. (A *lemma* in mathematics is a preliminary or auxiliary result, not the main result one is aiming at.)

LEMMA 2.1 (The Division Algorithm) If a and n are integers and n is positive, then there exist *unique* integers q and r such that $a = qn + r$ and $0 \leq r < n$ (q stands for quotient and r stands for remainder).

PROOF. We prove the existence of q and r, then the uniqueness.

q remainder r

n/a

Existence: Let qn be the greatest multiple of n that is $\leq a$. If we let $r = a - qn$ then clearly $r \geq 0$ and $a = qn + r$, so all we have to check is that $r < n$. But if $r \geq n$, then

$$r - n = a - (q+1)n \geq 0,$$

so $(q+1)n$ is a multiple of n that is $\leq a$, contradicting the choice of qn as the greatest such multiple.

Uniqueness: If $q_1 n + r_1 = q_2 n + r_2$ and $0 \leq r_1 < n$, $0 \leq r_2 < n$, then

$$q_1 n - q_2 n = r_2 - r_1,$$

so $r_2 - r_1$ is a multiple of n; but $-n < r_2 - r_1 < n$, so $r_2 - r_1 = 0$, so $r_2 = r_1$. Thus $q_1 n = q_2 n$, so $q_1 = q_2$. □

We denote the unique r guaranteed by the lemma by $\bar{a}$, and call it the **remainder of a mod n.**

Observe that two integers a_1 and a_2 have the same remainder mod n iff $a_1 - a_2$ is a multiple of n. When this happens, we say that a_1 and a_2 are **congruent modulo n,** and we write $a_1 \equiv a_2 \pmod{n}$.

Examples

By the lemma we can unambiguously define a binary operation $\oplus$ on $\mathbb{Z}_n$ by setting $x \oplus y = \overline{x+y}$.

We claim that this operation turns $\mathbb{Z}_n$ into a group $(\mathbb{Z}_n, \oplus)$.

Associativity: Read in book

Modern Algebra & Number Systems | Abstract_Algebra_1-5

(5) but $-n < r_2 - r_1 < n$ (4) by steps 2 and $r_i \in [0, n)$, $-r_1 \in (-n, 0]$, $r_2 - r_1 \in (-n, n)$

(6) So $r_1 - r_2 = 0 \cdot n$ (6) by steps 4+5

(7) So $r_1 = r_2$ (7) adding r_2 to both sides.

(8) $q_1 n = a - r_1$ $= a - r_2 = q_2 n$ (8) Step 2 subtracting r_i and step 7

(9) $q_1 = q_2$ (9) dividing by $n > 0$ □

1:25 AM Thu Aug 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

We denote the unique r guaranteed by the lemma by $\bar{a}$, and call it the **remainder of a mod n.**

Observe that two integers a_1 and a_2 have the same remainder mod n iff $a_1 - a_2$ is a multiple of n. When this happens, we say that a_1 and a_2 are **congruent modulo n,** and we write $a_1 \equiv a_2 \pmod{n}$.

Examples

By the lemma we can unambiguously define a binary operation $\oplus$ on $\mathbb{Z}_n$ by setting $x \oplus y = \overline{x+y}$.

We claim that this operation turns $\mathbb{Z}_n$ into a group $(\mathbb{Z}_n, \oplus)$.

Associativity: Read in book

Lets check $\mathbb{Z}_3$

22 **Section 2. Groups**

Identity: The identity element is 0. Why? $0 \oplus x = \overline{0+x} = \bar{x} = x$ if $0 \leq x \leq n-1$, and, similarly, $x \oplus 0 = x$.

Inverses: Read in book

The group $(\mathbb{Z}_n, \oplus)$ is called the additive group of integers mod n. Notice

Modern Algebra & Number Systems

Modern Algebra & Number Systems | Abstract_Algebra_1-5

Modular Arithmetic

$\mathbb{Z}_n = \{0, 1, 2, \ldots (n-1)\}$

$a \oplus b = (a+b) \bmod n$

where

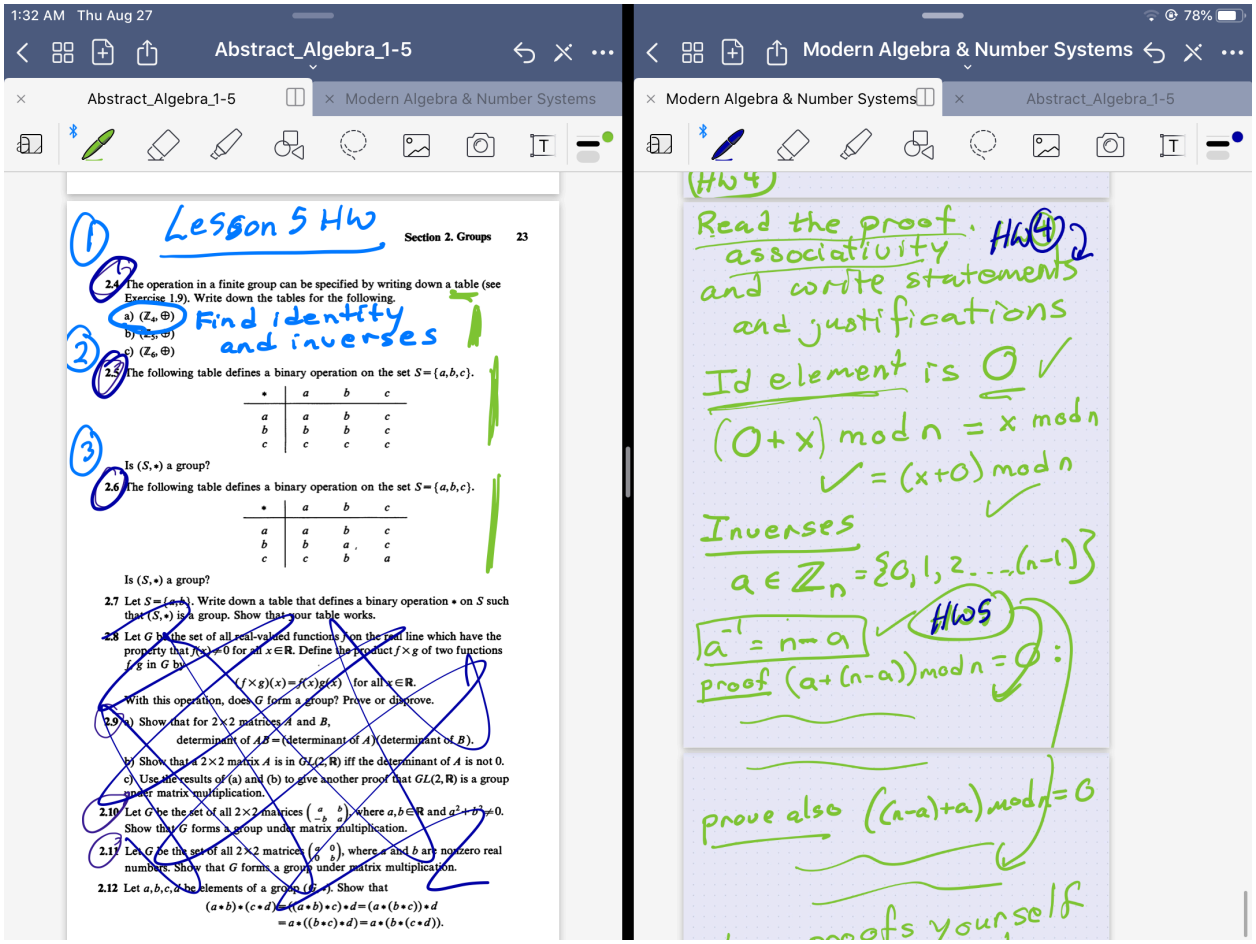
$x \bmod n$ for $x \in \mathbb{Z}$, $n \in \mathbb{N}$

is defined

$n \overline{)x}$ q remainder r

$x \bmod n = r$

book writes $\bar{x}$



HW6: Important for computer science students

Consider the set of two elements {p,q}. This set has four subsets

0 = empty set
{p}
{q}
{p,q}

Let S be the set of subsets.

Recall A/B= {x such that x is in A but x is not in B}
and
A union B= {x such that x in A or x in B}

Consider the operation symmetric difference defined on this set:

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

So this is the set {x such that x is in A but not B or x is in B but not A}

So for example:

$$\{p\} \triangle \{p\} = (\{p\} \setminus \{p\}) \cup (\{p\} \setminus \{p\})$$
$$= \emptyset \cup \emptyset = \emptyset$$

$$\{p,q\} \triangle \{p\} = (\{p,q\} \setminus \{p\}) \cup (\{p\} \setminus \{p,q\})$$
$$= \{q\} \cup \emptyset = \{q\}$$

$$\{p\} \triangle \{q\} = (\{p\} \setminus \{q\}) \cup (\{q\} \setminus \{p\})$$
$$= \{p\} \cup \{q\} = \{p,q\}$$

Write out the table of this symmetric difference as a binary operation for S. By set theory we know it is associative so you do not need to prove this. Find the identity and inverses to prove it is a group.

The HW is six problems given above. You need the textbook to complete the homework because you are now expected to be able to read the book and follow the proofs yourself as has been done in all the first five lessons. These problems are very similar to the classwork. Always try the classwork yourself before watching the solutions because that is your opportunity to see hints.

Another hint: if asked to check if something is a group or not, the quickest way is to check it is a binary operation first, then find the identity, then find the inverses, and only check associativity last. A more general hint: any time you are told to prove or disprove something with many things to check, check the easiest parts first.

Another hint: As explained on the lesson, check if (G,*) is a group you must prove all four of the following:
1.To prove binary operator as in lesson 4:
Given a,b in G show a*b in G
step 1 given a,b in G say what you know about a and b justify with defn of G
step 2 a*b= fill in justify with defn of *
step 3 = simplify it more if necessary and justify with something appropriate
step 4 conclude a*b in G justify by checking all the rules about G
2.To prove associativity in a finite group with a table you must check all combinations of x*(y*z)=(x*y)*z
aaa bbb ccc
aab aba baa
aac aca caa
abb bab bba
abc bac bca
cba cab acb
bbc bcb cbb
acc cac cca
and so on if there are even more elements.
3.To prove Identity you must check on both sides.
4.To prove Inverses you must check on both sides.
To show it is not a group you just need to show it fails one of the four points.

A statement in a proof needs to say something that is either true or false it cannot be left hanging: "a*b=" alone is not a statement.

Justifications are not explanations why you are doing something or your plans for what is going on. Each is a pure explanation why its statement is true. If no algebra is happening in the statement then the justification is not "algebra". If there is no matrix multiplication in the statement then the justification is not "matrix multiplication".

Once you have completed this homework and the professor has checked it you may start practicing the sample exam.

-------- The following message regarding Exam 1 was emailed to the class-------

For those of you who are completing Lesson 5 this week, you may take Exam 1 on Sunday or Monday. The rest of you may take the exam next week. Choose your preferred time at the top

of your google doc. Choose a time when your home is quiet. This is why I include a time in the middle of the night.

When you are sitting and ready to take the exam with your googledoc open to Lesson 6, send me an email. I will put part 1 of your individual exam in your google doc. You will complete that part within 30 minutes and upload the photos right below your exam. You may take a break and then email me you are ready for part 2 and we repeat. The googledoc will record the time when your photos were uploaded. You should also keep your photos.

Everyone has a different exam. All exams are similar to the samples. You may consult notes and the internet and use calculators or MATLAB or Maple but must show all work and must use the techniques taught in our class. You may not seek help from a human being or online tutoring service.

The 30 minutes for each part is a serious time limit. I need an official note from disability services to grant more time. If anyone panics during the exam, we will cancel the exam and you will take a new one the following week. If you have already completed part 1, you may cancel just part 2.

Remember you will only take this exam if you are ready for it. The goal is to get a perfect score on Exam I because the rest of the course builds on this material. Remember as always do not reply to this email, use sormanic@gmail.com.

Best Regards,

Prof Sormani