MATH 3330 ABSTRACT ALGEBRA SPRING 2014

TANYA CHEN

Dr. Gordon Heier

Tuesday January 14, 2014

The Basics of Logic (Appendix)

Definition. A statement is a declarative sentence that is either true or false.

Examples

(1) $\#\{4, \pi, 7, 3\} = 3$

(2) There is a real number x such that $x^2 = -1$.

(3) There exists infinitely many prime numbers.

Some statements are plainly assumed to be true. These are called postulates or axioms.

Examples

(1) One can draw a straight line through any two points in the plane.

(2) $3 < 4$

Most statements are derived from basic postulates by logical inference ("Theorems, proofs").

Quantifiers will often be used in our statements:
$\forall$: "for all"
$\exists$: "there exists"

(1) $\forall x \in (0, 2) : x > -3$ True
(2) $\exists x \in \mathbb{Z} : x^2 = 9$ True
(3) $\exists x \in \mathbb{Z} : x^2 = 10$ False
(4) $\forall a \in \mathbb{R} : \exists x \in \mathbb{R} : x^2 = a$ False
(5) $\forall a \in \mathrm{C} : \exists x \in \mathrm{C} : x^2 = a$ True

$\forall a \in \mathbb{R} : \exists x \in \mathbb{R} : x^2 = a$ is false. Prove statement (4) via a counterexample.
$-1 \in \mathbb{R}$, but $\forall x \in \mathbb{R} : x^2 \geq 0 > -1$

The logical opposite or "negation" of statement 4 is:
$\exists a \in \mathbb{R}\ \forall x \in \mathbb{R} : x^2 \neq a$

Example from Calculus:
$f : \mathbb{R} \to \mathbb{R}$ is continuous at $x_0 \Leftrightarrow \forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in (x_0 - \delta, x_0 + \delta) : |f(x) - f(x_0)| < \varepsilon$

$f : \mathbb{R} \to \mathbb{R}$ is *not* continuous at $x_0 \Leftrightarrow \exists \varepsilon > 0\ \forall \delta > 0\ \exists x \in (x_0 - \delta, x_0 + \delta) : |f(x) - f(x_0)| \geq \varepsilon$

From give statements, we can get new statements with "and," "or," "$\Rightarrow$," "$\Leftrightarrow$".

Examples

- $x > 3$ and $x < 5$
  (same as/"equivalent to" $x \in (3, 5)$)

- $x > 1$ and $x < 0$ False.

Today, Math 3330 meets for class $\Rightarrow$ Today is Tuesday.

This is one big statement: Today Math 3330 meets for class $\Rightarrow$ Today is Tuesday. False.

Today Math 3330 meets for class $\Leftarrow$ Today is Tuesday. True.

How to Negate With And/Or:
Let A and B be statements. Not(A and B) is the same as not A or not B.

Contrapositive
$A \Rightarrow B$ is equivalent to not $A \Leftarrow$ not B.

Green sweater $\Rightarrow$ Thursday

Chapter 1 Fundamentals

§1.1 Sets

$\{0, 2, 5, 7\} = \{0, 0, 2, 5, 5, 7, 7, 7\}$
$\# = 4$
Sets do *not* come with a notion of multiplicity of membership.

list, collection

Subset: $\{2,3\} \subset \{2,3,7,8\}$
$\subset :\Leftrightarrow \subseteq$
$\subset$
$\subsetneq$

$A \subset A$ True.
$\{1,3\} \not\subset \{2,3,7,8\}$

Equality of sets: $A = B \Leftrightarrow A \subset B$ and $B \subset A$

Thursday January 16, 2014

- TA office hours MF 12–12:50pm
- HW1 on website early afternoon.

§1.1 Sets (Continued)

\cup
$A \cup B = \{x | x \in A \text{ or } x \in B\}$

\cap
$A \cap B = \{x | x \in A \text{ and } x \in B\}$

Example.
$A = \{1, 5, 9\} \quad B = \{5, 7\}$
$A \cup B = \{1, 5, 7, 9\}$

$A \cap B = \{5\}$

Clear: $A \cup B = B \cup A$

Empty set: $\varnothing$ ({ })
$\{1, 2\} \cap \{3, 4, 5\} = \varnothing$

Important Notion: Complement
If $A, B \subset U$ (U is universal superset), $A^c := U \setminus A = \{x \in U | x \notin A\}$

$A \setminus B = \{x \in A | x \notin B\}$

Example. $U = \mathbb{Z}$, $A = \{\text{even integers}\}$, $B = \{\text{positive integers}\}$
$A^c = \{\text{odd integers}\} = \{\ldots, -5, -3, -1, 1, 3, \ldots\}$

$A \setminus B = \{0, -2, -4, -6, \ldots\}$

Repeated Application:

$$\begin{aligned}(A \cap B) \cap C &= A \cap (B \cap C) \\ &= A \cap B \cap C\end{aligned}$$

$\ni x \Leftrightarrow x \in A$ and $x \in B$ and $x \in C$.

Warning: $A \cap (B \cup C) \neq (A \cap B) \cup C$

Ex 14. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

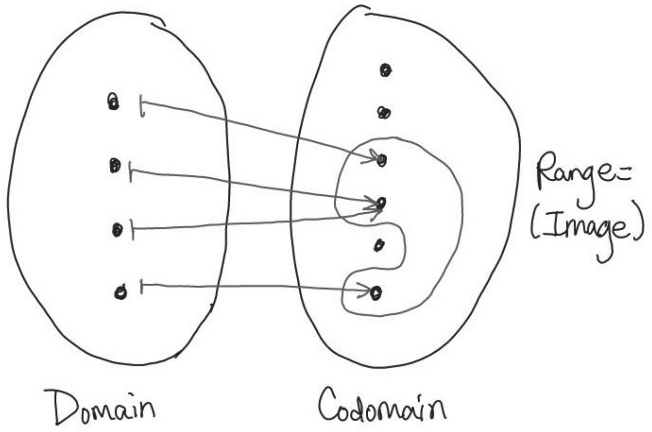
Proof. " $\subset$ " Let $x \in A \cap (B \cup C)$

$$\begin{aligned}
&\Rightarrow x \in A \text{ and } (x \in B \text{ or } x \in C)\\
&\Rightarrow (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C)\\
&\Rightarrow x \in A \cap B \text{ or } x \in A \cap C\\
&\Rightarrow x \in (A \cap B) \cup (A \cap C)
\end{aligned}$$

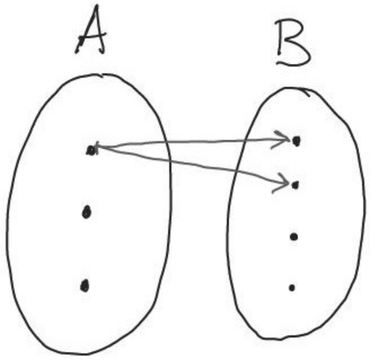
" $\supset$ " Reverse arrows for this direction. □

§1.2 Mappings

$$f : A \to B$$



Illegal:



Example. $f : \{1, 2, 3, 4\} \to \{1, 2, 3, \ldots, 20\}$
$x \mapsto x^2$

Domain: $\{1,2,3,4\}$
Codomain: $\{1,2,\ldots,20\}$
Range: $\{1,4,9,16\}$

Some more terminology: Let $f : A \to B$, let $S \subset A$.
Then $f(S) = \{f(x) | x \in S\} = \{b \in B : \exists x \in S : f(x) = b\}$.

Let $T \subset B$. Let $f : \mathbb{Z} \to \mathbb{Z}$. $x \mapsto x^2$.
$f^{-1}(T) = \{a \in A | f(a) \in T\}$
$\mathbb{Z}$ integers from German word Zahlen.

$f^{-1}(\{4,9\}) = \{-2,-3,2,3\}$
$f^{-1}(\{5,7,9\}) = \{\pm 3\}$
$f^{-1}(\{3\}) = \varnothing$

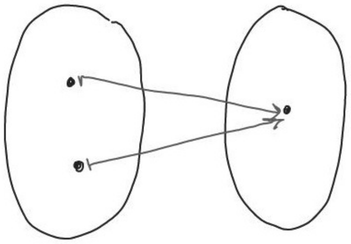
Injective Maps

Definition. Let $f : A \to B$ map. Then f is called injective if $\forall x, y \in A$ with
$x \neq y : f(x) \neq f(y)$
$\longrightarrow x \neq y \Longrightarrow f(x) \neq f(y)$

$$\boxed{x = y \Longleftarrow f(x) = f(y)}$$

$A \Rightarrow B$ same as not $A \Leftarrow$ not B

Not injective:



Example 1. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 3x + 2$

$f(x) = f(y)$
$\longrightarrow 3x + 2 = 3y + 2$
$\longrightarrow 3x = 3y$
$\longrightarrow x = y$

Thus f is injective.

Example 2. $f : \mathbb{Z} \to \mathbb{Z}$ $x \mapsto x^2$

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Not injective.
$f(-2) = 4 = f(2)$ but $-2 \neq 2$

Example 3. $f : \mathbb{N} \to \mathbb{N}$, $x \mapsto x^2$
Injective.

Surjective Maps:

Definition. Let $f : A \to B$ map. Then f is called <u>surjective</u> $\Leftrightarrow f(A) = B \iff$ codomain range $\iff \forall b \in B : \exists a \in A : b = f(a)$.

$\mathbb{R} \to \mathbb{N}$

$\mathbb{N} \to \mathbb{R}$

Examples

(1) $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto x^2$ Not surjective.

(2) $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ Not surjective because all squares of reals are non-negative. So $-2 \notin f(\mathbb{R})$.

(3) $f : \mathbb{R} \to (0, \infty), x \mapsto x^2$ Not a function.

(4) $f : \mathbb{R} \to [0, \infty), x \mapsto x^2$

(5) $f : \mathbb{R} \to \mathbb{R}, x \mapsto 3x + 2$ is surjective.

Proof. Let $y \in \mathbb{R}$ ($\mathbb{R}$ is codomain.)
Q: $\exists x \in \mathbb{R} : y = f(x)$? ($\mathbb{R}$ is domain.)

Solve.

$$\begin{aligned} y &= f(x) = 3x + 2 \\ \implies y - 2 &= 3x \\ \implies \frac{y-2}{3} &= x \end{aligned}$$

Check: $f\left(\frac{y-2}{3}\right) = 3\left(\frac{y-2}{3}\right) + 2 = y - 2 + 2 = y$

Tuesday January 21, 2014

$$x \mapsto \begin{cases} 2x+1 & \text{if } x \text{ is even.} \\ \dfrac{x+1}{2} & \text{if } x \text{ is odd.} \end{cases}$$

(a) Injective? Prove.
(b) Surjective? Prove.

Solution:

(a) Even:

x	$f(x)$
-2	-3
0	1
2	5
4	9

Odd:

x	$f(x)$
-3	-1
-1	0
1	1
3	2

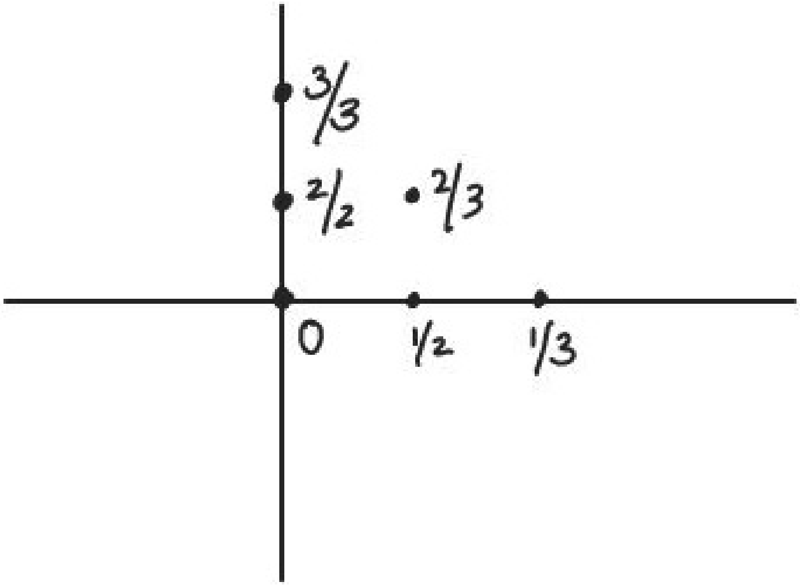
Not injective

(b) Let $y \in \mathbb{Z}$ arbitrary. $\exists x \in \mathbb{Z} : f(x) = y$

Claim. $\exists x \in \mathbb{Z}$ with x odd: $f(x) = y \iff \dfrac{x+1}{2} = y$. Then, $x = 2y - 1$ Then $f(2y-1) = \dfrac{2y}{y} = 2y$.

Indeed odd.

§1.4 Binary Operations



Cantor's Diagonal Count

$\mathbb{N} \to \mathbb{Q}$
$\mathbb{Z} \to \mathbb{Q}$

Definition. A binary operation on a non-empty set A is a mapping $f : A \times A \to A$.

$$(a_1, a_2) \mapsto f(a_1, a_2) = a_1 * a_2$$

Recall:$A \times B : \{(a, b) | a \in A, b \in B\}$.

Example. $x * y$

(1) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$(x, y) \mapsto x + y$

(2) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$(x, y) \mapsto x \cdot y^2$

(3) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$(x, y) \mapsto x^2 + y^2$

(4) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$(x, y) \mapsto 1 + x \cdot y$

(5) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$(x, y) \mapsto \dfrac{x \cdot y}{3}$

(6) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$
$(x, y) \mapsto \dfrac{x \cdot y}{3}$

Not a binary operation.

$f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$
$(x, y) \mapsto \dfrac{x \cdot y}{3}$

Definition. If $a_1 * a_2 = a_2 * a_1$ $\forall a_1, a_2 \in A$ then say f is commutative.

Definition. If $(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$ $\forall a_1, a_2, a_3 \in A$ then say f is associative.

Ex. Look at 3. $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x, y) \mapsto 1 + x \cdot y$

$1 + xy = 1 + yx \implies f$ is commutative.

x	1
y	2
z	3

$x * (y * z) = 1 * (2 * 3) = 1 * (1 + 2 \cdot 3) = 1 * 7 = 1 + 1 \cdot 7 = 8$
$(x * y) * z = (1 + 1 \cdot 2) * 3 = 3 * 3 = 1 + 3 \cdot 3 = 10 \neq 8$

$\implies$ Not associative.

Closedness

Let $f : A \times A \to A$ be a binary operation. If $B \subset A$ is $b_1 * b_2 \in B$ such that $\forall b_1, b_2 \in B$, then we say B is closed under $*$ in A.

$f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$
$\quad (x, y) \mapsto x + y$

Identity Element
Definition. $e \in A$ is called an identity element if $\forall x \in A : e * x = x = x * e$.

Examples

(1) $A = \mathbb{Z}$, $* = +$
$e = 0$

(2) $A = \mathbb{Z}$,$* = \cdot$
$e = 1$

(3) $A = \mathbb{Z}$, $x * y = x + y - 3$
$e = 3$
$e * x = 3 + x - 3 = x$ ✓
$x * e = x + 3 - 3 = x$ ✓

(4) $A = \mathbb{Z}$, $x*y = x$ has no identity element because $e*y = e$ but should be y.

(5) $A = \mathbb{Z}$, $x * y = 1 + xy$

$$e * y = 1 + ey = y \quad e * y = y$$
$$\Leftrightarrow ey = y - 1$$
$$\Leftrightarrow e = \frac{y-1}{y}$$

$y \neq 0$

Depends on y, which it must not.

Right inverse, left inverse, inverse.

Key: Need to have identity element present to start with.

$1 \cdot x = x \quad x \cdot 1 = x$

1 is identity element of $\cdot$ on $\mathbb{Z}$ or $\mathbb{Q}$ on $\mathbb{R}$.

Now, it makes sense to seek, given x, an element y, such that $x \cdot y = 1$.

Thursday January 23, 2014

§1.4 Binary Operations (continued)

Recall: e is neutral $\Leftrightarrow \forall x \in A : e * x = x = x * e$

Assume e exists.

Definition. Right inverse, left inverse, inverse.

Let $a \in A$.

- if $\exists b \in A : a * b = e$ call b right inverse of a.
- If $\exists b \in A : b * a = e$, then call b left inverse of a.
- If $\exists b \in A : a * b = e = b * a$ then call b inverse of a.

Ex 1. $\mathbb{R}^{\neq 0} \times \mathbb{R}^{\neq 0} \to \mathbb{R}^{\neq 0}$
$(x, y) \mapsto x \cdot y$
$e = 1$ inverse to x is $\frac{1}{x}$.

Ex 2. $\mathbb{R}^{>0} \times \mathbb{R}^{>0} \to \mathbb{R}^{>0}$
$(x, y) \mapsto x(y^2)$
1 ✗ 1 ✓
No e thus no way to discuss any kind of inverse.

Ex 3. $\mathbb{R}^{\neq 0} \times \mathbb{R}^{\neq 0} \to \mathbb{R}^{\neq 0}$
$(x, y) \mapsto 3 \cdot xy$

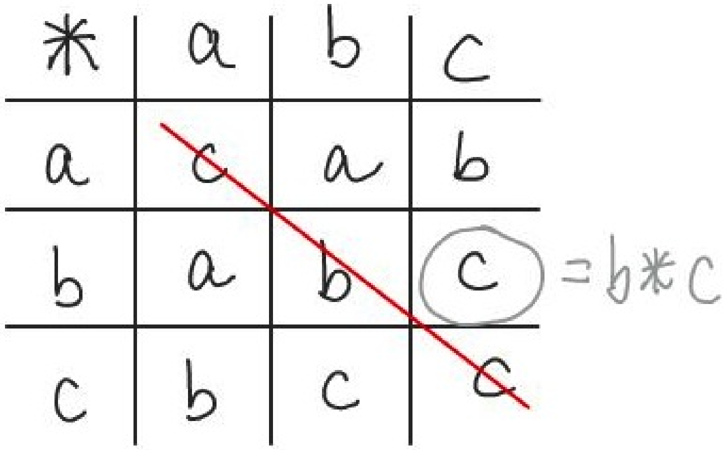
$\boxed{e = \frac{1}{3}}$ because

$$\frac{1}{3} \cdot y = 3 \cdot \frac{1}{3} \cdot y = y$$

$$x \cdot \frac{1}{3} = 3 \cdot x \cdot \frac{1}{3} = x$$

Inverse of a is b such that $a * b = e = 1/3$
$\frac{1}{9a}$
$a * b = e = 1/3$
$3ab \Leftrightarrow b = \frac{1}{9a}$

Ex 4. 1^{st}



*	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

= b*c

$$* : A \times A \mapsto A$$

(a) comm?
(b) $\exists\ e$? $e =$?
(c) $\exists$ inverses?

$a_i * a_j$
$A = \{a_1, \ldots, a_n\}$

$$a_i * a_j = a_j * a_i$$
$$(i,j)\text{–square} \quad (j,i)\text{–square}$$

(a) Yes, $*$ is commutative because the table is symmetric.
(b) $b * x = x$ and $x * = x \Longrightarrow b = e$
(c) inverse: $b * b = b = e \Longrightarrow b$ is its own inverse.

$x * y = x$
$y * x = x$

The inverse of c is a.
The inverse of a is c.

§1.5 Permutations

Let A be a set. (*Not* necessarily finite!)

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$A = \{1, 2, 3\}$

Definition. A bijective map $f : A \to A$ is called a permutation on A.

$S(A) = \{\text{permutations}\}$
$M(A) = \{\text{all maps } A \to A\}$

Composition of maps yields a binary operation on $S(A)$.
It also yields binary operation on $M(A)$.

$e =?$

$$\begin{array}{|c|}\hline \text{e} \\ \hline 1 \\ \hline \end{array}$$

$* : M(A) \times M(A) \to M(A)$

$e = id_A$

Left-inverses? Right-inverses? Inverse
e

Given $f \in M(A)$, $\exists?$ $g \circ f = id_A$.

Theorem. Let $f \in M(A)$. Then f injective $\Leftrightarrow$ f has a left inverse.

Proof. "$\Rightarrow$": Proof by explicit construction: the left inverse g.
For $a_2 \in$Range(f) $\exists$ unique element $a_1 \in A$.

$$f(a_1) = a_2$$

For $a_2 \notin$ Range(f) set $g(a_2) =$ some arbitrary $a \in A$ (does *not* matter which one). Check that g is left inverse

$$(g \circ f)(a) = g(f(a)) = a$$

□

"$\Leftarrow$" Let g be left-inverse. Let $f(a_1) = f(a_2)$. Need to show $a_1 = a_2$.

Apply g to both sides:

$$\begin{array}{ccc} \Longrightarrow g(f(a_1)) & = & g(f(a_2)) \\ id(a_1) & & id(a_2) \\ a_1 & & a_2 \end{array}$$

□

Thursday January 30, 2014

- HW2 now due 2/4 (Tuesday)
- Selected solutions to HW1 this afternoon on my www.

§1.5 Permutations

Let A any set.
Definition. $f : A \to A$ is called a <u>permutation</u> $\Leftrightarrow$ f bijective.

$S(A) = \{\text{permutations}\}$
$\cap$
$M(A) = \{\text{all } f : A \to A\}$

For $g, f \in M(A)$,

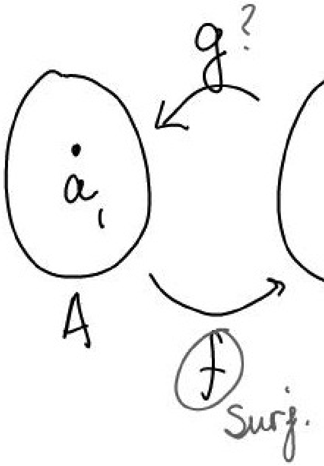
$$f * g = f \circ g$$

$e = Id_A$.

Theorem. Let $f \in M(A)$. Then f <u>injective</u> $\Leftrightarrow$ $\exists$ <u>left-inverse</u> of f.

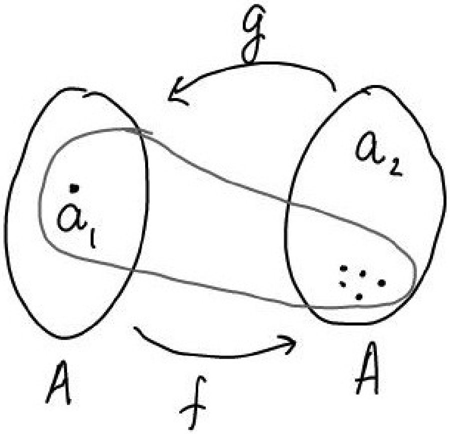
Right-inverse:
Theorem. Let $f \in M(A)$. Then f surjective $\Leftrightarrow$ $\exists$ right-inverse of f.

Proof. "$\Longrightarrow$" Take $a_2 \in A$. Since f surjective $\Longrightarrow \exists a_1 \in A : f(a_1) = a_2$.



$id = f \circ g \Longleftrightarrow$: g is a right-inverse of f.

Let $g(a_2) := a_1$. (Any element a such that $f(a) = a_2$ will do.)



Claim: g *is* a right inverse of f.
Proof of Claim: $(f \circ g)(a_2) = f(g(a_2)) = f(a_1) = a_2$ □

"$\Longleftarrow$" Take $a_2 \in A$ arbitrary. Let $a_1 := g(a_2)$ with g right-inverse.

Observe: $f(a_1) = f(g(a_2)) = id(a_2) = a_2$ □

Remark: Just saw: f bijective $\Leftrightarrow$ f has an inverse.

Example 1. $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 3x$.

$3x = 3y$

- f is not surjective, thus no right inverse.
- f is injective.

  g ? is a left-inverse.

  $$x \mapsto \begin{cases} \frac{x}{3} & \text{if } x \in 3\mathbb{Z} \qquad \{..., -9, -6, -3, -, 3, 6, 9, ...\} \\ 0 & \text{otherwise. does not matter.} \end{cases}$$

  g such that $g \circ f = id$.

- $x \mapsto \begin{cases} \frac{x}{2} & \text{if } x \text{ even.} \\ \text{x+2} & \text{if } x \text{ odd.} \end{cases}$
- f is *not* injective: $f(1) = 3 = f(6)$.

- f is surjective: a right-inverse of f is $g : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$.
  $(f \circ g)(x) = f(g(x)) = f(2x)$

Example 3. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$.
f is not injective.
f is not surjective.

Left-inverse: g such that $g \circ f = id$.
"$\sqrt{x}$ does not work for $x < 0$."

$x * y = e$

§1.7 Relations

A (~~binary~~) relation on a set A is a subset $R \subset A \times A$. If $(a, b) \in R_1$, write $a \sim b$.

Example 1. $A = \{1, 2, 3\}$. $R = \{(1, 1), (2, 2), (3, 3)\}$
Note: $(a, b) \in R$ $(:\Leftrightarrow a \sim b) \Leftrightarrow a = b$.

Example 2. Same A. $R = \{(1, 2), (2, 3), (1, 3)\}$

Example 3. Let A be any set. Let $R = \{(a, f(a)) | a \in A\}$. R is the graph of $f : a \sim b \Leftrightarrow b = f(a)$.

Definition. Let A be a set. The relation R is called an equivalence relation $\Leftrightarrow$

(1) $\forall x \in A : x \sim x$ (Reflexive)

$A = \{1, 2, 3\}$
$R = \{(1, 2), (1, 3), (2, 3), (7, 1), (3, 1), (3, 7)\}$
$(a, b) \in R \Leftrightarrow a \neq b$.
$a \sim b \Leftrightarrow a \neq b$.
( ),( )

(2) $\forall x, y \in A : x \sim y \Longrightarrow y \sim x$ (Symmetric)

(3) $\forall x, y, z \in A : (x \sim y \text{ and } y \sim z) \Longrightarrow x \sim z$ (Transitive)

$a < b, b < c \Longrightarrow a < c$

Ex 1. $A = \mathbb{Z}, a \sim b \Leftrightarrow |a| = |b|$.

Reflexive ✓

Proof. Let $a \in A$. Have to check $a \sim a$ is true. $a \sim a \Leftrightarrow |a| = |a|$. True. □

Symmetric ✓

Proof. Let $a \sim b \Longrightarrow |a| = |b| \Longrightarrow |b| = |a| \Longrightarrow b \sim a$ □

Transitive ✓

Proof. Let $a \sim b$, $b \sim c \Longrightarrow |a| = |b|, |b| = |c| \Longrightarrow |a| = |c|$. □

All three ✓, equivalence relation.

Ex 2. $A = \mathbb{Z}, a \sim b \Leftrightarrow a = |b|$.

Reflexive ✗
Let $a = -1$. Then $a \sim a$ is false: $-1 = |-1| = 1$✗.

Symmetric ✗
$a = 1, b = -1$. $a \sim b \Leftrightarrow 1 = |-1| = 1$. ✓
Check: $b \sim a \Leftrightarrow -1 = |1| = 1$. ✗

Transitive left as exercise.

$A = \mathbb{Z}$. $\sim$ is "congruence mod m." It IS an equivalence relation.

$$x \sim y \Leftrightarrow \exists k \in \mathbb{Z} : x - y = km$$

e.g. $m = 2$

Definition. Let R be an equivalence relation on A.

$$[a] := \{x \in A : x \sim a\}$$

is called the equivalence class of A.

Tuesday February 4, 2014

Quiz 2

(1) Let $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 7x$.

   (a) $\exists$ left-inverse? If yes, find it.
   (b) $\exists$ right-inverse? If yes, find it.

(2) Let $x, y \in \mathbb{Z}$. Let $x \sim y \Leftrightarrow x^2 + y^2$ is a multiple of 2. Equivalence relation?

Theorem. Let $f \in M(A)$. Then f $\underline{\text{injective}} \Leftrightarrow \exists$ $\underline{\text{left-inverse}}$ of f.

Theorem. Let $f \in M(A)$. Then f $\underline{\text{surjective}} \Leftrightarrow \exists$ $\underline{\text{right-inverse}}$ of f.

(1a) $x \mapsto \begin{cases} \frac{1}{7}x & \text{if } x \in 7\mathbb{Z} \\ 0 & \text{if } x \notin 7\mathbb{Z} \end{cases}$

(1b) Not surjective.

(2) R is reflexive and symmetric. For transitivity,

$$\text{True} \begin{cases} \exists k \in \mathbb{Z} : x^2 + y^2 = 2k \\ \exists k \in \mathbb{Z} : l \in \mathbb{Z} : y^2 + z^2 = 2l \end{cases}$$

$$\exists k \in \mathbb{Z} \exists l \in \mathbb{Z} : x^2 - z^2 = 2k - 2l = 2(k - l)$$

This is unchanged by adding the even number $2z^2$. $\implies x^2 - z^2 + 2z^2 = x^2 + z^2$ is even. $\square$

$$\mathbb{Q} \qquad \frac{a}{b} \qquad \begin{matrix} (a, b) \\ (1, 2) \\ (2, 4) \end{matrix}$$

$(a, b) \sim (c, d) \Leftrightarrow ad = bc$.

Recall: Equivalence classes. Let R equivalence relation on A. Then $[a] := \{x \in A : x \sim a\}$ is called the equivalence class of a.

$A = \mathbb{R}$

Ex 1. $x \sim y \Leftrightarrow |x| = |y|$
$[\pi] = \{\pi, -\pi\}$

$\boxed{\mathbb{Z}_n}$

Ex 2. Congruence mod 3 (recall: $x \sim y \Leftrightarrow x - y = 3k$ for some $x, y, k \in \mathbb{Z}$)

$[0] = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$
$[1] = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$
$[2] = \{\dots, -10, -7, -4, -1, 2, 5, 8, \dots\}$

$[12] = [-9] = [0] = \dots$

Theorem. Let R be an equivalence relation on A. Let $a, b \in A$. Then, either $[a] = [b]$ or $[a] \cap [b] = \varnothing$

Proof. Assume $[a] \cap [b] \neq \varnothing$. Need to show: $[a] = [b]$. Let $x \in [a] \cap [b]$ (exists!)
Let $\hat{a} \in [a]$.

Claim: $\hat{a} \in [b]$.
Have: $\hat{a} \sim a$

$$\begin{aligned} &x \sim a \\ &x \sim b \\ &\Downarrow \\ &\hat{a} \sim b \\ &\Downarrow \\ &\hat{a} \in [b] \end{aligned}$$

Thursday February 6, 2014

Recall: Let R be an equivalence relation on A.
Let $a \in A$. $[a] := \{x \in A | x \sim a\}$.

Theorem. Let $[a]$, $[b]$ be two equivalence classes. Then either $[a] = [b]$ or $[a] \cap [b] = \varnothing$.

Proof. Assume $[a] \cap [b] \neq \varnothing$. Need to show $[a] = [b]$.
Let $x \in [a] \cap [b]$.
Let $\hat{a} \in [a]$.

Claim: $\hat{a} \in [b]$.
Note: $\hat{a} \sim a, a \sim x, x \sim b \Rightarrow \hat{a} \sim x$

Not official language $\hat{a} \sim \cancel{a}, \cancel{a} \sim x, x \sim b \Rightarrow \hat{a} \sim x$
$\hat{a} \sim x, x \sim b \Rightarrow \hat{a} \sim x$

$\therefore \Rightarrow$ By transitivity, $\hat{a} \sim b$. ☐

§2.2 Mathematical Induction

Principle of Mathematical Induction

Let P_n be a statement depending on $n \in \mathbb{N} = \{0, 1, 2, \dots\}$ (or perhaps $\mathbb{N} = \{1, 2, 3, \dots\}$ at our convenience.)

If P_0 is true and $(P_n \Rightarrow P_{n+1})$ is true, then $\forall n \in \mathbb{N} : P_n$ is true.

Example. Gauss's trick:

1	2	3	$\cdots$	100
100	99	98	$\cdots$	1
101	101	101	$\cdots$	101

$101 + 101 + 101 + \cdots + 101$

$$\frac{100 \cdot 101}{2} = 5050$$

Example. $$P_n : \sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Let us prove P_n for $n = 1, 2, 3, \dots$ (i.e. for all $n \in \mathbb{N}$) by mathematical induction.

$P_1 : \quad 1 = \dfrac{1 \cdot (1+1)}{2}$ ✓

Now, need to prove that $P_n \to P_{n+1}$.

Claim: $P_{n+1} :\ 1 + 2 + \ldots + n + n + 1 = \dfrac{(n+1)(n+2)}{2}$

Prove this under the assumption that P_n holds, i.e. $1 + \ldots + n = \dfrac{n(n+1)}{2}$.

$$(1 + \ldots + n) + (n+1) \overset{\substack{P_n \text{ is true.} \\ \downarrow}}{=} \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2}$$
$$= \frac{(n+1)(n+2)}{2} \qquad \square$$

Example. $2^1 + 2^2 + 2^3 + \cdots + 2^n = 2(2^n - 1)$.

$P_1 : 2^1 = 2(2^1 - 1)$ ✓

"$P_n \Rightarrow P_{n+1}$": $(2^1 + 2^2 + 2^3 + \cdots + 2^n) + 2^{n+1} = 2(2^n - 1) + 2^{n+1} = 2(2^n - 1 + 2^n) = 2(2 \cdot 2^n - 1) = 2(2^{n+1} - 1)$ $\square$

Example. $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2 - 1)$

$P_1 : 1^3 = 1^2(2 \cdot 1^2 - 1)$ ✓

$P_n \Rightarrow P_{n+1}$:

Claim. $(1^3 + 3^3 + \cdots + (2n-1)^3) + (2(n+1) - 1)^3 = (n+1)^2(2(n+1)^2 - 1)$

LHS (using P_n): $n^2(2n^2 - 1) + (2(n+1) - 1)^3 \underset{\substack{\uparrow \\ \text{Brute force}}}{=} 2n^4 + 8n^3 + 11n^2 + 6n + 1$

RHS: $(n+1)^2(2(n+1)^2 - 1) = 2n^4 + 8n^3 + 11n^2 + 6n + 1$

Principle of Generalized Induction

Let $a \in \mathbb{N}$. If P_a is true and ($P_n \Rightarrow P_{n+1}$ is true $\forall n \in \mathbb{N}$ with $n \geq a$, then $\forall n \in \mathbb{N}$ with $n \geq a :\ P_n$ is true.

Example. $\forall n \geq 4 :\ 1 : 3n < n^2$

Proof. (By Generalized Induction)

$P_4 : \quad 1 + 3 \cdot 4 < 4^2$ ✓

"$P_4 \Rightarrow P_{n+1}$":

$P_{n+1} : 1 + 3(n+1) < (n+1)^2$

$$1 + 3(n+1) = 1 + 3n + 3 < n^2 + 3 \underset{\overset{\uparrow}{n \geq 4}}{<} n^2 + \boxed{2n+1} = (n+1)^2 \qquad \square$$

Principle of Complete Induction

Let $a \in \mathbb{N}$. If P_a is true and $(P_a, P_{a+1}, \dots, P_n \Rightarrow P_{n+1})$ all assumed to be true, then $\forall n \in \mathbb{N}$ with $n \geq a :\ P_n$ is true.

$123 = 1 \cdot 10^2 + 2 \cdot 10 + 3 \cdot 10^0$

Theorem. Every positive integer can be written in base 2, i.e. $\forall n \in \mathbb{N} \geq 1\ \exists j \in \mathbb{N} \geq 1\ \exists c_0, \dots, c_{j-1} \in \{0, 1\} : n = c_0 \cdot 2^0 + c_1 2^1 + c_2 2^2 + \cdots + c_{j-1} 2^{j-1} + 2^{j-1}$

Proof. Let $j = 1$. Let $c_0 = 1$.

$1 = 1 \cdot 2^0$. ✓

"$P_1, \dots, P_n \Rightarrow P_{n+1}$"

Case 1. n even ($\Leftrightarrow n + 1$ odd)

$$P_n \Rightarrow \underset{\overset{\uparrow}{\text{even}}}{n} = \underset{=0 \text{ b/c } n \text{ even}}{\boxed{c_0 \cdot 2^0}} \quad + \underset{\overset{\uparrow}{\text{even}}}{c_1 2} + \underset{\overset{\uparrow}{\text{even}}}{c_2 2^2} + \cdots + \underset{\overset{\uparrow}{\text{even}}}{c_{j-1} 2^{j-1}} + \underset{\overset{\uparrow}{\text{even}}}{2^j}$$

add $+1$

$\longrightarrow n + 1 = 1 + c_1 2 + \cdots + c_{j-1} 2^{j-1} + 2^j$

Case 2. n odd ($n + 1$ even).

let $k = \dfrac{n+1}{2}$.

$P_k \Rightarrow k = \tilde{c_0} \cdot 2^0 + \tilde{c_1} 2 + \cdots + \tilde{c}_{j-1} 2^{j-1} + 2^j$

Multiply by 2:

$n + 1 = 2k = \tilde{c}_0 2^1 + \tilde{c}_1 2^2 + \tilde{c}_2 2^3 + \cdots + \tilde{c}_{j-1} 2^j + 2^{j+1}$

Set $c_0 = 0$.

$c_i = \tilde{c}_{i-1}$ for $i = 1, \ldots j$

Tuesday February 11, 2014

Quiz 3

(1) $\forall n \in \mathbb{N}^{\geq 3}: \; 1+2n < 2^n$
(2) $\forall n \in \mathbb{N}^{\geq 1}: \; 1^3+2^3+\cdots+n^3 = \frac{1}{4}n^2(n+1)^2$

(1) First, $n = 3$. ✓. Then the induction step: $1+2n+2 < 2^n+2 < 2^n+2^n = 2\cdot 2^n = 2^n+1$
Replace 2 with 2^n. □

(2) Assume P_n is true. Show LHS in P_{n+1} = RHS in P_{n+1}.

$$\frac{1}{4}n^2(n+1)^2+(n+1)^3 = (n+1)^2(\frac{1}{4}n^2+(n+1))$$
$$= \frac{1}{4}(n+1)^2(n^2+4n+4) = \frac{1}{4}(n+1)^2\cdot(n+2)^2$$

§2.3 Divisibility

Recall. For $b \in \mathbb{Z}$, $a \in \mathbb{Z}\setminus\{0\}$, $a|b$ (say "a divides b") $\Leftrightarrow\; \exists c \in \mathbb{Z} : b = c\cdot a$

Recall. The division algorithm / division with remainder.
Let $a, b \in \mathbb{Z}$, $b > 0$. Then $\exists! q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ with $r \in \{0,1,\ldots,b-1\}$. $a = q\cdot b + r$.

Example. $a = 3, b = 10$. $q = 3, r = 5$ and $35 = 3\cdot 10+5$ or $a = q\cdot b+r$.

$a = 72$, $b = 7$. $72 = 10\cdot 7+2$.

$a = -91$, $b = 11$.

Observe. $-91 = \underset{\uparrow}{\boxed{(-8)\cdot 11 - 3}} = (-9)11+8$

Not a valid division with remainder.

$-91 = (-9)11+10$
$a = qb+r$

Recall. Long division algorithm.
$a = 357, b = 13$. $\frac{357}{13} = 27$ with remainder: 6.

For negative a how to do long division with remainder: Work with $|a|$, then multiply by (-1), then adjust to positive remainder.

Example. $a = -122$, $b = 11$.
First, work with $+122 : \dfrac{122}{11} = 11$ with remainder 1.

$122 = 11 \cdot 11 + 1$

Multilpy by $(-1) : \underset{a}{-122} = (-11)11 - 1 = \underset{q}{(-12)} \cdot \underset{b}{11} + \underset{r}{10}$

§2.4 Prime Factors and GCDs (Greatest Common Divisors)

Definition. $d = \gcd(a, b)$ such that $a, b \in \mathbb{Z}$ if and only if:

1. $d \in \mathbb{N}^{\geq 1}$ (i.e., d positive integers)
2. $d|a$, $d|b$
3. $c|a$ and $c|b \Rightarrow c|d$

Theorem. (GCD-Theorem)

Let a, b be integers, at least one non-zero. The <u>smallest</u> non-zero $d \in \mathbb{N}^{\neq 0}$ that can be written as $d = am + bn$ with $m, n \in \mathbb{Z}$ in the $\gcd(a, b)$.

1. Show: $d|a$ ($d|b$ by symmetry)
   We can always divide a by d with remainder: $a = q \cdot d + r$ if and only if

   $$\begin{aligned} r &= a - qd = a - q(am + bn) \\ &= a - q(am + bn) \\ &= a(1 - mq) + b(-nq) \end{aligned}$$

   Note: This shows that r has the same property of d, but d was *smallest* (and $r < d$). $\rightarrow\leftarrow$ unless $r = 0$.

2. Remains: There is no greater divisor than d. To this end, let c be any other divisor.
   $d = \underset{c \cdot l_1}{a}m + \underset{c \cdot l_2}{b}n = cl_1m + cl_2n = c(l_1m + l_2n) \Rightarrow c|d$ □

How to find m, n, d for given a, b? Let $a, b \in \mathbb{N}$.

Key idea: Subtracting a multiple of the smaller number (either a, b) from the other number does *not change* the GCD.

Thursday February 13, 2014

GCD Theorem. Let $a, b \in \mathbb{Z}$. The smallest non-zero $d \in \mathbb{N}^{\neq 0}$ that can be written

$$d = am + bn \quad (m, n \in \mathbb{Z})$$

is the GCD.

Note. $d = am + bn = (-a)(-m) + bn$

Key idea. Subtracting a multiple of the smaller number from the larger number where a, b are the numbers, does not change the GCD.

Example. Find $\gcd(1492, 176)$.

$$\begin{aligned}
\gcd(1492, 176) &= \gcd(1492,\ 1776 - 1492 = 284)\\
&= \gcd(1492 - 5 \cdot 284 = 72,\ 284)\\
&= \gcd(72,\ 284 - 3 \cdot 72 = 68)\\
&= \gcd(72 - 1 \cdot 68 = 4,\ 68)\\
&= 4 \text{ (obviously)}
\end{aligned}$$

Scratch Work. $1492 = 5 \cdot 284 + 72$
$4 \cdot 72 = 288$

Example. To find m, n such that $4 = 1492 \cdot m + 1776 \cdot n$.

$$\begin{aligned}
4 &= 72 - 68 = 72 - (284 - 3 \cdot 72) =\\
&= 4 \cdot 72 - 284 = 4(1492 - 5 \cdot 284) - 284\\
&= 4 \cdot 1492 - 21 \cdot 284\\
&= 4 \cdot 1492 - 21 \cdot (1776 - 1492)\\
&= 25 \cdot 1492 + (-21)1776\\
&\quad\ m \qquad\qquad\quad n
\end{aligned}$$

Example. $a = 102, b = 66$.

$$\begin{aligned}
\gcd(102, 66) &= \gcd(102 - 66 = 36,\ 66)\\
&= \gcd(36,\ 66 - 36 = 30)\\
&= \gcd(36 - 30 = 6,\ 30)
\end{aligned}$$

$$\begin{aligned}
6 &= 36 - 30\\
&= (102 - 66) - (66 - 36)\\
&= 102 - 2 \cdot 66 + 36
\end{aligned}$$

$$\begin{aligned} &= 102 - 2 \cdot 66 + 102 - 66 \\ &= 2 \cdot 102 + (-3)66 \end{aligned}$$

$$\quad m \qquad\qquad n$$

Remark. For next section, $3a = 3b$. Most would conclude $a = b$.   mod 3 is true for all $a, b \in \mathbb{Z}$.

Definition. Call a, b relatively prime $\Leftrightarrow$ $\gcd(a, b) = 1$.

Definition. An integer $p > 1$ is called prime if $a|p \Rightarrow a = \pm 1$ or $a = \pm p$.

Euclid's Lemma. If p prime and $p|a \cdot b \Rightarrow p|a$ or $p|b$.
(Consider $5|10 \cdot 7$)

Unique Factorization Theorem.

Every positive integer > 1 can be expressed as a product of primes, unique up to reordering of the factors.

Proof. By complete induction. If n is prime, done. If not, write $n = a \cdot b$ where $a > 1$ and $b > 1$. Apply induction twice, once to a and once to b. (Both are $< n$.) ☐

Euclid's Theorem on Primes. There exists infinitely many primes.

Proof. To obtain a contradiction, let us assume that $p_1, \ldots, p_k$ for $k \in \mathbb{N}$ is a complete list of all primes. Consider: $m = p_1 + \ldots + p_k + 1$. Note $m > p_i \ \forall i = 1, \ldots, k \Rightarrow m$ is not a prime. Unique Factorization Theorem $\Rightarrow$ $\exists i : p_i | m$. But the remainder obtained when dividing m by p_i is obviously 1. ↯ ☐

Example. Find prime factorization in an ad-hoc way.

$$\begin{aligned} 84 &= 2 \cdot 42 = 2^2 \cdot 21 \\ &= 2^2 \cdot 3 \cdot 7 \end{aligned}$$

Remark. This yields an alternative way of finding the GCD.

$\gcd(287, 161)$ can be determined as follows:

$$\begin{aligned} 287 &= \boxed{7} \cdot 41 \\ 161 &= \boxed{7} \cdot 23 \\ \Rightarrow \ \gcd &= 7. \end{aligned}$$

$$1492 = \underset{\substack{\uparrow\\ 2^2}}{4} \cdot \underset{\substack{\uparrow\\ \text{prime}}}{373},\ \ 1776 = 2^4 \cdot 3 \cdot 37$$

§2.5 Congruence of Integers

Remark. Let $a, b \in \mathbb{Z}$. $a \equiv b \mod n \in \mathbb{N}^{>0} \Leftrightarrow \exists k \in \mathbb{Z} : a - b = k \cdot n$.

Remark. "$\equiv \mod n$" is an equivalence relation.

Proof.

1. Reflexive: $a - a = 0 \cdot n$
2. Symmetric: $a - b = k \cdot n \Rightarrow b - a = -kn = (-k) \cdot n$
3. Transitive: $a \cdot b = k_1 n$ and $b - c = k_2 \cdot n \Rightarrow a - (k_2 n + c) = k_1 n \Rightarrow$ $a - c = k_1 n + k_2 n = (k_1 + k_2)n$
   $b = k_2 n + c$ $\square$

Theorem (2.22) Let x be any integer.

(a) $a \equiv b \mod n \ \Leftrightarrow\ a + x \equiv b + x \mod n$ Reversible
(b) $a \equiv b \mod n \ \Rightarrow\ xa \equiv xb \mod n$ Not Reversible

Proof. (a) Let $a \equiv b \mod n$, i.e., $\exists k \in \mathbb{Z} : a - b = kn$.

Check: $a + x - (b + x) = a - b = kn$
$a + \cancel{x} - (b + \cancel{x}) = a - b = kn$ ✓
(b) $xa - xb = x(a - b) = x(kn) = (xk)n$ ✓

Theorem 2.23 $a \equiv b \mod n$ and $c \equiv d \mod n \Rightarrow a + c = b + d \mod n$

Proof. $a + c - (b + d) = a - b + c - d = k_1 \cdot n + k_2 \cdot n = (k_1 + k_2) \cdot n$
$k_1 + k_2 \in \mathbb{Z}$ $\square$

Tuesday February 18, 2014

Quiz 4

(1) $\gcd(117, 315) = ?$

$$\gcd(117, 315) = \gcd(81, 117) = \gcd(81, 36) = \gcd(36, 9) = 9$$

(2) Find $m, n \in \mathbb{Z} : \gcd(117, 315) = m315 + 117n$

$$\begin{aligned} 9 &= 81 - (2 \cdot 36) \\ &= 81 - 2 \cdot (117 - (1 \cdot 81)) \\ &= (3 \cdot 81) - (2 \cdot 117) \\ &= 3(315 - (2 \cdot 117)) - (2 \cdot 117) \\ &= 3 \cdot 315 - 8 \cdot 117 \\ \therefore m &= 3,\ n = -8 \end{aligned}$$

§2.5 Congruence of Integers (Continued)

$(a, b \in \mathbb{Z})$

$$\begin{aligned} a \sim b &:\Leftrightarrow a \equiv b \mod n \\ &:\Leftrightarrow \exists k \in \mathbb{Z} : a - b = kn \end{aligned}$$

is an equivalence relation.

Theorem. For any $x \in \mathbb{Z}$,

(1) $a \equiv b \mod n \Leftrightarrow a + x \equiv b + x \mod n$
(2) $a \equiv b \mod n \Rightarrow ax \equiv bx \mod n$

$$\Leftarrow ↯$$

Theorem. $a \equiv b \mod n$
$c \equiv d \mod n$
$\Rightarrow a + c \equiv b + d \mod n$.

Theorem 2.24 (Cancellation Law)
If $ax \equiv ay \mod n$ and $\gcd(a, n) = 1$ then $x \equiv y \mod n$.

Proof. $ax \equiv ay \mod n$
$\Leftrightarrow \exists k : k \cdot n = (ax - ay)$
$\Leftrightarrow n|(ax - ay)$
$\Leftrightarrow n|(a(x - y))$
$\Leftrightarrow n|x - y$
$\gcd(a, n) = 1$
$\Leftrightarrow x \equiv y \mod n$ ☐

Remark. What goes wrong if $\gcd(a, n) > 1$:

$2 \cdot 2 \equiv 2 \cdot 4 \mod 4$
$a \quad x \quad a \quad y \qquad n$
$\gcd(a, n) = \gcd(2, 4) = 2 \neq 1$
"cancel" the factor of 2:
$2 \equiv 4 \mod 4$
$x \quad y \quad \lightning$

Want to solve two types of equations:

1. $ax \equiv b \mod n$ with $\gcd(a, n) = 1$ (solve for x).
2. $x \equiv a \mod m$.
   $x \equiv b \mod n$
   $(\gcd(m, n) = 1)$
   Solve for x.
   $\boxed{\text{all over } \mathbb{Z}}$

Theorem 2.25. Let $a, b, n \in \mathbb{Z}$. Let $\gcd(a, n) = 1$. Then the congruence $ax \equiv \mod n$ has a solution $x \in \mathbb{Z}$ *and* any two solutions are congruent mod n.

Proof. $\gcd(a, n) \underset{\substack{\uparrow \\ \text{GCD Theorem}}}{=} 1 \Rightarrow \exists s, t \in \mathbb{Z} : 1 = as + nt$

$ax \equiv \mod n \Leftrightarrow \exists k \in \mathbb{Z} : ax - b = kn$

$\gcd(a, n) = 1 \Rightarrow \underset{\text{Multiply by } b}{\underline{\exists s, t \in \mathbb{Z} : 1 = as + nt}}$

$\Rightarrow \exists s, t \in \mathbb{Z} : b = a(bs) + n(bt)$
$\Rightarrow \exists s, t \in \mathbb{Z} : a(bs) - b = n(-bt)$

$\Rightarrow \exists s, t \in \mathbb{Z} : a\underset{x}{\underline{(bs)}} - b = n\underset{\in \mathbb{Z}}{\underline{(-bt)}}$

Finally, let us determine all solutions. Let x, y both solve the congruence equation.

$$\left.\begin{aligned} ax &\equiv b \mod n \\ ay &\equiv b \mod n \end{aligned}\right\}$$

$$\Rightarrow \cancel{a}x \equiv \cancel{a}y \mod n$$
$$\uparrow \text{Transitivity of } \equiv$$

$\Rightarrow x \equiv y \mod n$
$\uparrow$ Cancellation Law

□

Example. $20x \equiv 14 \mod 63$.
Note: $\gcd(20, 63) = 1$.

Write $\quad 1 = 20(-22) + 63(7)$
$(b = 14) \cdot 1 \quad 14 = (20(-22)14) + 63(7 \cdot 14)$

$$14 = (20\underbrace{(-22)14}_{x=-308}) + 63(7 \cdot 14)$$

What is the smallest positive x which solves?
$-308 + 5 \cdot 63 = 7$

Check your answer: $20 \cdot 7 - 14 = 2 \cdot 63$ ✓

$3x \equiv 7 \mod 13$
$1 = 3s + 13t$
$1 = 3(-4) + 13t$
$7 \cdot 1 \quad 7 = 3(-28) + 13 \cdot 7$
$x = -28 \qquad$ smallest positive $x = 11$

Theorem 2.26. Let $\gcd(m, n) = 1$.
Let $a, b \in \mathbb{Z}$.
Then $\exists x \in \mathbb{Z} : x \equiv a \mod m \quad (1)$
$x \equiv b \mod n \quad (2)$
Any two solutions x, y are congruent $\mod m \cdot n$.

Proof. Solve (1): $x = a + mk \quad \forall k \in \mathbb{Z}$.
Solve into (2): $a + mk \equiv b \mod n$
$\Leftrightarrow \boxed{mk \equiv b - a \mod n}$

Since $\gcd(m, n) = 1$, Theorem 2.2.5 $\Longrightarrow$ Can solve for k. ($\rightarrow$ Get k_0.)
$x = a + mk_0$ solves (1) and (2). □

Uniqueness to congruence mod m, n

Let x, y be two solutions.

$x \equiv a \mod m \qquad y \equiv a \mod m$
$x \equiv b \mod n \qquad y \equiv b \mod n$

$x \equiv y \mod m$

$x \equiv y \mod n$

$m|x-y$
$m|x-y$

$m \cdot n|x-y$

Thursday February 20, 2014

Recall. Let $a, b, n \in \mathbb{Z}$ with $\gcd(a, n) = 1$. $\Rightarrow \exists x \in \mathbb{Z} : ax \equiv b \mod n$. Any two solutions x, y are congruent mod n.

Let $a, b \in \mathbb{Z}$. Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. $\Rightarrow \exists x \in \mathbb{Z} : x \equiv a \mod m$ and $\equiv b \mod n$. Any two solutions x, y are congruent mod $m \cdot n$.

Example. $x \equiv 2 \mod 5 \qquad (1)$
$x \equiv 3 \mod 8 \qquad (2)$

$(1) \Leftrightarrow x = 2 + 5k$

Sub into (2): $2 + 5k \equiv 3 \mod 8 \Leftrightarrow 5k \equiv 1 \mod 8$.

Find s, t such that $1 = 5s + 8t$.

$\gcd(5, 8) = \gcd(5, 3) = \gcd(3, 2) = 1$

$$\begin{aligned} \Rightarrow 1 &= 3 - 2 \\ &= (8 - 5) - (5 - 3) \\ &= 8 - 2 \cdot 5 + 3 \\ &= 8 - 2 \cdot 5 + (8 - 5) \\ &= 2 \cdot 8 + (-3)5 \\ &\qquad\quad -3 = s = k \\ &\rightarrow x = 2 + 5(-3) = -13 \end{aligned}$$

Smallest positive x is $-13 + 40 = 27$.

Check. $27 \equiv 2 \mod 5$ ✓
$27 \equiv 3 \mod 8$ ✓

Example. $\boxed{2}x \equiv \boxed{5} \mod \boxed{3} \qquad (1)$
$5x + 4 \equiv 5 \mod \boxed{7} \qquad (2)$

Solve (1). $1 = 3 - 2 \qquad 1 \cdot 5$
$5 \cdot 1 = 5 \cdot 3 + 2\underset{x}{\boxed{(-5)}}$
$x = -5 + 3k = 1 + 3k$

Substitute into (2). $5(1 + 3k) + 4 \equiv 5 \mod 7$
$\Leftrightarrow 15k + 9 \equiv 5 \mod 7$

$$\begin{aligned} &\Leftrightarrow \boxed{15}k \equiv \underline{-4} \mod \boxed{7} \\ &1 = 15 + (-2)\cdot 7 \qquad 1\cdot(\underline{-4}) \\ & \\ &-4 = (\underset{k}{\underline{-4}})15 + 8\cdot 7 \end{aligned}$$

$x = 1 + 3(-4) = -11$

Smallest positive $x = -11 + 21 = 10$

Check. $2\cdot 10 \equiv 5 \mod 3$ ✓
$50 + 4 \equiv 5 \mod 7$ ✓

Let $a, b \in \mathbb{Z}$.
Let $m, n \in \mathbb{Z}$ with $\gcd(m,n) = 1$.
$\Rightarrow \exists x \in \mathbb{Z} : x \equiv a \mod m$
$x \equiv b \mod n$
Any two solutions x, y are congruent mod $m \cdot n$.

Theorem 2.2.7 (Chinese Remainder Theorem)

Let $n_1, \dots, n_m$ pairwise relatively prime. Let $a_1, \dots, a_m \in \mathbb{Z}$.

$$\begin{aligned} \Rightarrow \exists x \in \mathbb{Z} : \; & x \equiv a_1 \mod n_1 \\ & x \equiv a_2 \mod n_2 \\ & \quad \vdots \\ & x \equiv a_m \mod n_m \end{aligned}$$

Any two solutions are congruent mod $n_1 \cdot \ldots \cdot n_m$.

§2.6 Congruence Classes

$$\begin{aligned} \mathbb{Z}_n &= \{\text{congruence classes of integers } \mod n\} \\ &= \{[0], [1], [2], \dots, [n-1]\} \end{aligned}$$

$[0] = \{\dots, -2n, -n, 0, n, 2n, \dots\}$
$[2] = \{\dots, 2-2n, 2-n, 2, 2+n, 2+2n, \dots\}$

Define addition on $\mathbb{Z}_n : [a] + [b] = [a+b]$

Note. This *is* well-defined because:

$$\begin{aligned} [a+rn] + [b+sn] &= [a+rn+b+sn] \\ &= a+b+n(r+s) \\ &= [a+b] \end{aligned}$$

Associativity $([a]+[b])+[c]=[a]+([b]+[c])$ ✓

Commutativity: $[a]+[b]=[b]+[a]$ ✓

Identity: $[0]+[a]=[a]$ ✓
$[-a]+[a]=[0]$ ✓

Table for $\mathbb{Z}_4=\{[0],[1],[2],[3]\}$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Multiplication: $[a]\cdot[b]=[ab]$
Commutativity ✓
Associativity ✓
Identity: [1]

Multiplication Table for $\mathbb{Z}_4$

•	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	**[0]**	[2]
[3]	[0]	[3]	[2]	[1]

$$[2]\cdot[2]=[0]$$

Start with a, n.
Let's study multiplicative inverses:

$$[a]\cdot[b]=[1]$$

$\Leftrightarrow [ab-1]=[0]$
$\Leftrightarrow \exists q\in\mathbb{Z}: ab-1=qn$
$\Leftrightarrow \exists q\in\mathbb{Z}: a\cdot b+(-q)n=1$

GCD Theorem $\Rightarrow b$ (and q) exist $\Leftrightarrow \gcd(a,n)=1$.

Just saw: $[a]$ has multiplicative inverse in $\mathbb{Z}_n \Leftrightarrow \gcd(a,n)=1$.

Corollary. Every element of $\mathbb{Z}_p$ has a multiplicative inverse if $p =$ prime.

Let's solve equations (system of equations) in $\mathbb{Z}_n$:

Example. $[4]\cdot[x]=[5]$ in $\mathbb{Z}_{13}$
$[4]^{-1}\cdot| \quad [x]=[4]^{-1}[5]$

Remains to find $b:[b]=[4]^{-1}$:

b	$\cdot[4]$
0	0
1	$[4]$
2	$[8]$
3	$[12]$
4	$[3]$
5	$[7]$
6	$[11]$
7	$[2]$
8	$[6]$
9	$[10]$
$\boxed{10}$	$\boxed{[1]}$

$\Rightarrow [4]^{-1}=[10]$
$\Rightarrow [x]=[4]^{-1}\cdot[5]=[10]\cdot[5]=[50]=[11]$

28-26=2
32-26-6
36-26=10
40-39=1

Tuesday February 25, 2014

Quiz 5

(1) $5x + 1 \equiv 3 \mod 13$
(2) $x \equiv 3 \mod 5$
$2x \equiv 5 \mod 7$

In each case, find *all* solutions.

Example. $[4][x] + [y] = [22]$ in $\mathbb{Z}_{26}$.
$[19][x] + [y] = [15]$

Subtract (2) from (1):

$$[-15][x] = [7]$$
$$\Leftrightarrow [11][x] = [7]$$
$$\Leftrightarrow [x] = [11]^{-1} \cdot [7]$$

To find $[11]^{-1}$:

$$\boxed{x \cdot 11 \equiv 1 \mod 26}$$

$$\boxed{ax \equiv b \mod m}$$

$1 = 11 \cdot s + 26t$
$s = -7$, $t = 3$

$11 \cdot 19 = 110 + 99$
$209 \cdot 26 = 8$
$208/1$

$z = -7$
$\Rightarrow [11]^{-1} = [-7] = [19]$
$\Rightarrow [x] = [19] \cdot [7] = [133] = [3]$

Remains: $[4] \cdot [3] + [y] = [22]$
$\Leftrightarrow [y] = [22] - [12] = [10]$

§3.1 Definition of a group.

Definition. A group in a set G and a binary operation $* : G \times G \to G$ such that

(1) $*$ is associative, i.e., for all $x, y, z \in G : (x * y) * z = x * (y * z)$
(2) There exists an identity element e, i.e., there exists $e \in G$ such that for all $x \in G$ it follows $e * x = x = x * e$.

(3) For all $a \in G$, there exists $b \in G$ such that $a*b = e = b*a$ ("existence of inverses")

Definition. If G is a group with $x, y \in G$, and $x * y = y * x$, then call G abelian or commutative.

Examples.
$(\mathbb{Z}, +)$ is a commutative group.
$(\mathbb{Z}, \cdot)$ not a group.
(3) fails: No multiplicative inverses (except for ± 1).

$(\mathbb{R}, +)$ ✓
$(\mathbb{R}, \cdot)$ is not a group $\left(\text{“}\frac{1}{0}\text{”} \text{ is a problem.}\right)$
$(\mathbb{R} \setminus \{0\}, \cdot)$ is a group.

Thursday February 27, 2014

§3.1 Definition of a *Group*

Let G be a set with binary operation $*$.

1. $*$ is associative.
2. There exists an identity element.
3. For all $a \in G$, $\exists b \in G$ such that $a * b = e = b * a$.

If, in addition, $*$ is *commutative*, then G is called Abelian or commutative.

Example 1. $(\mathbb{R}, +), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{Z}, +)$

Example 2. $G = \{f : \mathbb{R} \to \mathbb{R} \text{ continuous}\}$ with $(f+g)(x) = f(x) + g(x)$.
$+$ is a binary operation because of the summation theorem for continuous functions and satisfies (1), (2), (3).

Example 3. $A = \{1, 2, 3\}$
$\rho(A) = \{f : A \to A\}|\text{bijective}\}$

$$\rho(A) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{if } x < 0. \end{cases}$$

$*$	e	α	β	γ	σ	ε
e	e	α	β	γ	σ	ε
α	α	β	e			
β	β					
γ	γ					α
σ	σ					
ε	ε					

$$\begin{aligned} &1 \mapsto 2 \\ \alpha \circ \alpha : {}&2 \mapsto 3 \\ &3 \mapsto 1 \end{aligned}$$

$$\begin{aligned} &1 \mapsto 1 \\ \alpha \circ \beta : {}&2 \mapsto 2 \\ &3 \mapsto 3 \end{aligned}$$

$$\begin{aligned} &1 \mapsto 3 \\ \gamma \circ \varepsilon : {}&2 \mapsto 1 \\ &3 \mapsto 2 \end{aligned}$$

Example 4. $\#G = 2 \Rightarrow G \cong (\mathbb{Z}_2, +)$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Example 5. $\#G = 3 \Rightarrow G \cong (\mathbb{Z}_3, +)$

Example 6. $\#G = 4$

(a) $G = (\mathbb{Z}_4, +)$

(b)

$*$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	$\boxed{b}$	a	e

↑

$aba = b\cancel{aa}$

$G = \{e, a, b, ab\}$ G abelian with $a * a = e$
$b * b = e$
$(ab) * (ab) = e$

We will see: G in $\mathbb{Z}_2 \times \mathbb{Z}_2$
$(AB)^{-1}$
Felix→ (Klein's Four Group)

§3.2 Properties of Group Elements

Theorem 3.4

(a) $e \in G$ is unique.
(b) For all $x \in G$ the universe of x is unique (thus the special x^{-1} can be used).
(c) For all $x \in G : (x^{-1})^{-1} = x$
(d) For all $x, y \in G : (xy)^{-1} = y^{-1}x^{-1}$
(e) For all $a, x, y \in G : (ax = ay \Rightarrow x = y)$

$x * y = xy$

Proof. (a) Let e, e' be neutral elements.

$$e \underset{\substack{\uparrow \\ e' \text{ neutral}}}{=} ee' \underset{\substack{\uparrow \\ e \text{ neutral}}}{=} e'$$

(b) Let $a \in G$. Let b, c both be inverses.

$$b = eb = (ca)b = c(ab) = ce$$

(c) $x^{-1} \cdot x = e$ ✓
$x \cdot x^{-1} = e$ ✓

(d) $$(xy)(y^{-1}x^{-1}) = x(\underset{\substack{\uparrow \\ yy^{-1} = e}}{yy^{-1}})x^{-1} = xx^{-1} = e$$

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

$$xyx^{-1}y^{-1}$$

(e) Let $ax = ay \mid a^{-1} *$

$$a^{-1}(ax) = a^{-1}ay \Leftrightarrow (a^{-1}a)x = (a^{-1}a)y \Leftrightarrow x = y$$

□

Remarks on Matrix Groups
$(Mat_{n\times m}(\mathbb{R}), +)$ is a group.
$(Mat_{n\times m}(\mathbb{R}), \cdot)$
$(Mat_{n\times m}(\mathbb{R}) | \{\det A = 0\}, \cdot) = GL_n\mathbb{R}$

§3.3 Subgroups

Definition. Let G be a group. A *subset* $H \subset G$ is called a *subgroup* if H is a group with the binary operation induced from G.

Equivalent Definition. $\varnothing \neq H \subset G$ is called a subgroup $\Leftrightarrow$

1. $x, y \in H \Rightarrow x * y \in H$
2. $x \in H \Rightarrow x^{-1} \in H$

Example 1. $H = \{[0], [2], [4]\} \subset (\mathbb{Z}_6, +)$

(1) ✓
(2) $[2]{-}1 = [4]$ ✓
$[4]^{-1} = [2]$ ✓
$\Rightarrow H$ is a subgroup of $(\mathbb{Z}_6, +)$
$[2] + [4] = [6] = [0] = e$

(3) $H = \{[0], [1], [2]\} \subset (\mathbb{Z}_6, +)$

$$\underset{\substack{\uparrow \\ H}}{[1]} + \underset{\substack{\uparrow \\ H}}{[2]} = [3] \notin H \Rightarrow H \text{ is not a subgroup of } \mathbb{Z}_6$$

Tuesday March 4, 2014

Online Tutoring: Tuesday 6-7pm
Fridays 1-2pm
www.math.ueh.edu/∼nleger

§3.3 Subgroups (continued)

Recall: $\varnothing \neq H \subset G$ (G for group) is a subgroup $\Leftrightarrow$

1. $x, y \in H \Rightarrow x * y \in H$
2. $x \in H \Rightarrow x^{-1} \in H$

$* : G \times G \to G$
$\quad H \times H \to H$

Examples (continued)

(1) $G = (\mathbb{R} \setminus \{0\}, \cdot)$ is a group.
$H = \{x \in \mathbb{R}, x > 0\}$
 (a) $\Leftrightarrow$ "The product of positive reals is positive." *True.*
 (b) $\Leftrightarrow$ "The reciprocal of a positive real is positive." *True.*
(a) and (b) $\Rightarrow$ H *is* a subgroup.

(2) $G = (\mathbb{R} \setminus \{0\}, \cdot)$
$H = \{x \in \mathbb{R}, x < 0\}$
 (a) $\Leftrightarrow$ "The product of negative reals is negative." *False.*
 H is *not* a subgroup.

(3) $G = (\mathbb{R} \setminus \{0\}, \cdot)$
$H = \{1, 2, 3, 4, 5, \ldots\}$
 (a) Any product of natural numbers is a natural number. ✓
 (b) For $x \in \{2, 3, 4, 5, \ldots\}$, $\frac{1}{x} \notin H$, i.e., condition (b) is *not* satisfied and H is *not* a subgroup.

(4) $G = (\mathbb{R} \setminus \{0\}, \cdot)$
$H = (\mathbb{Q} \setminus \{0\}, \cdot)$ ✓subgroup
$H = (\mathbb{Q} \setminus \mathbb{Z}, \cdot)$
Condition (a) does not hold. $\frac{2}{3} \cdot \frac{9}{2} = 3$.
So $\frac{2}{3} \in H$, $\frac{9}{2} \in H$, but $3 \notin H$.
✗*Not* a subgroup.

$H = \{1, -1\} \cong \mathbb{Z}_2$ ✓

(5) $A = \{1, 2, 3\}$
$\varphi(A) = \{\text{bijective maps } \{1,2,3\}\}$.

$$H = \{\text{id}\} \checkmark$$

$$H = \left\{ \text{id} \quad \alpha : \begin{array}{c} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{array} \quad \alpha \circ \alpha : \begin{array}{c} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{array} \right\}$$

(a) All we need to check is:

$$\alpha \circ \alpha \in H \checkmark$$

$$\alpha \circ (\alpha \circ \alpha) : \begin{array}{c} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{array} = \text{id} \in H \quad \checkmark$$

$$(\alpha \circ \alpha) \circ (\alpha \circ \alpha) : \begin{array}{c} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{array} = \alpha \in H \quad \checkmark$$

(b) $\alpha \cdot \alpha \in H \checkmark$
$\alpha \cdot (\alpha \cdot \alpha)$
$\alpha^{-1} = \alpha \circ \alpha \checkmark$
$(\alpha \circ \alpha)^{-1} = \alpha \checkmark$
$\Rightarrow H$ is a subgroup of $\varphi(A)$.

Integral Exponents

For $a \in G$, define:
$\forall k \in \mathbb{N} : a^k = \underbrace{a * (\ldots (a * (a * a)) \ldots)}_{k \text{ factors}}$
$\forall k \in \{-1, -2, -3, -4, \ldots\} : a^k = (a^{-1})^{(k)} = (a^{(k)})^{-1}$
$x \in \mathbb{R}* \qquad x^{-3} = \dfrac{1}{x^3} = \left(\dfrac{1}{x}\right)^3$

Theorem. (Laws of Exponents)

$m, n \in \mathbb{Z}$

(1) $x^n * x^{-n} = e$
(2) $x^m * x^n = x^{m+n}$
(3) $(x^m)^n = x^{m \cdot n}$
(4) If G abelian, then $(xy)^n = x^n y^n$

Cyclic (Sub)groups:

Definition. Let G be a group. Say G is cyclic. $\Leftrightarrow \exists a \in G : G = \underset{\substack{\downarrow \\ < a >}}{\{a^n | n \in \mathbb{Z}\}}$

Definition. Let G be a group. Let $H \subset G$. We call H a *cyclic subgroup of* G.
If $\exists a \in G :< a >= H$.

Definition. Any such a is called a generator of H (or G, respectively).

Example 1. $(\mathbb{Z}, +) =< 1 >=< -1 >$

$H = \{e\}$ Note: $1^3 = 3^0$
$1^3 = 3 \cdot 1$ $3^0 = 1 * 1 * 1$

Example 2. Consider $G = (\mathbb{Z}, +)$
$H =< 2 >= \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$ is the cyclic subgroup of $\mathbb{Z}$ generated by 2.

Example 3. $G = (\mathbb{Z}_6, +)$

$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$

Let's find all the cyclic subgroups of G.

$H =< [0] >= \{[0]\}$

$H =< [1] >= G$

$[1] = \{[0], [1], [1] + [1] = [2] \quad [2] + [1] = [3], \dots\}$

$H =< [2] >= \{[0], [2], [4]\}$

$H =< [3] >= \{[0], [3]\}$

$H =< [4] >= \{[0], [4], [2]\}$

$H =< [5] >= \{[0], [5], [4], [3], [2], [1], [0]\} = G$

Saw: $G =< [1] >=< [5] >$
$< [2] >=< [4] > \cong \mathbb{Z}_3$
$< [3] > \cong \mathbb{Z}_3$
$< [0] >= \{e\}$

Remark. Let G be a group. Then any group element $x \in G$ yields a cyclic group $< x >= \{x^n | n \in \mathbb{Z}\}$.

Thursday March 6 2014

Timetable:

Today in class: Q6 solution and new material.
Later today: New HW 7 on my www, due 03/18.
Class of 03/18: Solutions to HW 7 discussed in class. Further exam prep. No new material.
Class of 03/20: MT Exam
Sample exams: See my earlier Math 3330 on my www.

Theorem 3.15 Infinite Cyclic Groups

Let $a \in G$. If $a^n \neq e$ for all $n > 0$, then $a^p \neq a^q$ for all $p \neq q = \mathbb{Z}$ and $< a >$ is infinite cyclic.

Proof. If $a^p = a^q$ for $p \neq q$, then $a^{p-q} = e$ (without loss of generality $p > q$)
By assumption: $p - q = 0$ ↯

Corollary. If $\#G$, then $a^n = e$ for some $n \in \mathbb{N} > 0$.

Theorem 3.20 (Subgroups of Cyclic Groups)
Let G cyclic group with generator a. Let $H \subset G$ subgroup. Then either
a) $H = \{e\} =< e >$ or
b) $H =< a^k >$ where k is the least positive integer such that $a^k \in H$.

Proof. Let $b \neq e \in H$. Have to show: $\exists l \in \mathbb{Z} \neq 0 : b = a^{ek}$. Assume false.
Because $b \in G : \exists j : b = a^j$
Do division with remainder $j = m \cdot k + r$ with $0 < r < k$. Since H is a subgroup, $b \cdot (a^{mk})^{-1} \in H$.
a^r ↯ minimality of k.

Definition. The *order* (ord(a)) of $a \in G$ is $\# < a >$.
Clear: ord(a) $= \min\{m \in \mathbb{N} > 0 : a^m = e\}$

Department of Mathematics, University of Houston, Houston, TX, USA
E-mail address: `tgchen@uh.edu`