Proof Portfolio
MATH 347, Spring 2022

Shuzhen Zhang
Version: January 5, 2023

Contents

1 Common Theorems

This section will contain five theorems common to everyone.

1.1 Size of Power set

Theorem 1. *If* $|A| = n$*, then* $|\mathscr{P}(A)| = 2^n$.

Proof. Assume there is a set B which is the subset of A, and | A | = n.

Every elements in the A would have 2 different possibilities, which could also in the B or not.

so the total different subsets of A in terms of B would be 2^n;

since the $\mathscr{P}(A)$ is the all subset of A, $|\mathscr{P}(A)|$ will equal to the number of different set B which is 2^n.

□

1.2 Power set always bigger

Theorem 2. *Let A be a set. Then there is no surjection $g : A \to \mathscr{P}(A)$.*

Proof. Suppose $g : A \to \mathscr{P}(A)$ is surjective function.

Then $\forall y$ in $\mathscr{P}(A)$, there must exist a pre-image $x \in$ A, and $f(x) = y$.

we can get $f(x) \in \mathscr{P}(A) \to f(x) \subseteq \mathscr{P}(A)$

let define a set $C \subseteq \mathscr{P}(A)$ and

$$C = \{x \in A | x \notin f(x)\} \tag{1}$$

$\forall C \subseteq \mathscr{P}(A)$, there exist $x \in A : f(x) = C$.

Therefore, there are two situations here.
(1) if $x \in C$, $x \notin f(x) \to x \notin C$
(2)if $x \notin C$, $x \notin f(x) \to x \in C$
which generated contradiction statement; therefore, it is impossible for $g: A \to \mathscr{P}(A)$ contain surjection. □

1.3 Inverse exists and is invertible

Theorem 3. *Let $f: A \to B$ be an bijective function. Then there is a function $f^{-1}: B \to A$ has the property that*

$$f^{-1}(f(x)) = x \quad \forall x \in A, \quad f(f^{-1}(y) = y) \quad \forall y \in B,$$

AND *f^{-1} is an invertible function.*

Proof. since $f: A \to B$ is a bijective function, then $f(x) = f(z)$ if and only if $x = z$ and $\forall x, z \in A$.
let define there exist a function that $g: B \to A$, and let $g(y) = x, \forall y \in B$ and $\forall x \in A$.
then we got: $g(f(x)) = x$ and $f(g(y)) = y$
since f is bijective, so $g(f(x)) = g(y)$ is also bijective.
and we can see $g(y)$ just the invertible function of $f(x)$. □

1.4 Operations with modulos

Theorem 4. *Let Z_n be the set $\{0, 1, 2, \ldots, n-1\}$ where we define two operations $+_n$ and $*_n$ where*

$$x +_n y = (x + y) \pmod{n}, \quad x \times_n y = x \times y \pmod{n}.$$

Consider the relation on $\mathbb{Z}$ given by

$$x \sim y \iff x \equiv y \pmod{n}.$$

1. *Show that $\sim$ is an equivalence relation.*
2. *Let $[x]$ be the equivalence class of x under this relation. Prove that*

$$[x + y] = [x] +_n [y], \quad [x \times y] = [x] \times_n [y].$$

Proof. (1)
we can check the property of reflexive, symmetric, and transitive.
reflexive: $x \sim x$
$x \equiv x \pmod{n} \to x - x = kn, \forall k \in \mathbb{Z}$.
symmetric: $x \sim y$ and $y \sim x$
if $x \equiv y \pmod{n} \to x - y = kn, \forall k \in \mathbb{Z}$, then
$x - y = kn \to -(y - x) = kn \to y - x = -kn, y \equiv x \pmod{n} \forall k \in \mathbb{Z}$.
transitive: if $x \sim y$ and $y \sim z$, then $x \sim z$

let $x, y, z \in \mathbb{Z}$ and $x \sim y, y \sim z$, then
$x \equiv y \pmod{n} \rightarrow x - y = kn, \forall k \in \mathbb{Z}$ and
$y \equiv z \pmod{n} \rightarrow y - z = ln, \forall l \in \mathbb{Z}$
$x - y + y - z = kn + ln \rightarrow x - z = (k + l)n \rightarrow x \equiv z \pmod{n}$

□

Proof. (2)
let x' in equivalence class[x], we can obtain $x \sim x'$ and $x = x' + kn$, $k \in \mathbb{Z}$
let y' in equivalence class[y], we can obtain $y \sim y'$ and $y = y' + ln$, $l \in \mathbb{Z}$

$$x + y = x' + y' + (k + l)n \tag{2}$$

$$(x + y) \sim (x' + y') \tag{3}$$

since $(x' + y')$ is one element of $[x] +_n [y]$ in the equivalence class $[x + y]$,
$[x + y] = [x] +_n [y]$
let x' in equivalence class[x], we can obtain $x \sim x'$ and $x = x' + kn$, $k \in \mathbb{Z}$
let y' in equivalence class[y], we can obtain $y \sim y'$ and $y = y' + ln$, $l \in \mathbb{Z}$

$$x * y = (x' + kn) * (y' + ln) \tag{4}$$

$$\rightarrow x * y - x' * y' = x'ln + y'kn + kln^2 \tag{5}$$

$$\rightarrow x * y - x' * y' = (x'l + y'k + kln) * n \tag{6}$$

$$(x * y) \sim (x' * y') \tag{7}$$

since $(x' * y')$ is one element of $[x] *_n [y]$ in the equivalence class $[x * y]$,
$[x * y] = [x] *_n [y]$

□

1.5 Fibonacci

Definition. *Define the Fibonacci numbers* $(F_n)_{n \geq 1}$ *by:*

$$F_1 = 1, \quad F_2 = 1, \quad F_n = F_{n-1} + F_{n-2}.$$

Theorem 5. *The Fibonacci number F_n is even iff n is a multiple of 3.*

Proof. Let proof by induction:
Base case:
At n=3,$F_3 = F_2 + F_1 = 1 + 1 = 2$, base case passed;
Induction process:

suppose F_n is divisible by 2 for n= 3,6,9...,3k-3,3k , $k \in \mathbb{Z}$
$F_{3k+3} = F_{3k+2} + F_{3k+1}$
$= F_{3k} + F_{3k+1} + F_{3k-1} + F_{3k}$
$= 2F_{3k} + F_{3k} + F_{3k-1} + F_{3k-2} + F_{3k-3}$
since $F_{3k} = F_{3k-1} + F_{3k-2}$
$= 2F_{3k} + F_{3k} + F_{3k} + F_{3k-3}$
since F_{3k} and F_{3k-3} both divisible by 2, F_{3k+3} is divisible by 2;
Therefore, for all F_n is divisible by 2 iff n is a multiple of 3.

$\square$

2 My own theorems

This chapter will contain five theorems chosen by you.

2.1 Tricky GCD

Theorem 6. *gcd(2n, n + 1) = 2 when n is odd,and gcd(2n, n + 1) =1 when n is even.*

Proof. since we need to proof something with GCD, let's reform it by Euclidean theorem.

$$2n = 1 * (n+1) + (n-1) \tag{8}$$

$$n+1 = 1 * (n-1) + 2 \tag{9}$$

then, do one more step

$$(n-1) = 2 * q + r \tag{10}$$

$r \in [0,1]$,so there are two cases:

case1: if $r = 0$, $n-1$ must be an even, n must be an odd. Moreover the Non-zero remainder would be 2.

case2: if $r = 1$, $n-1$ must be an add, n must be an even. The remainder is 1.

□

2.2 Closed form Of Taylor Series

Theorem 7. *for* $\sum_{i=0}^{n} \frac{1}{2^i} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} ...... + \frac{1}{2^n}$, *there exist a closed form that* $\sum_{i=0}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}$.

Proof. Let proof by induction: at n=0

$$\sum_{i=0}^{n} 1/(2^i) = 1/(2^0) = 1/1 = 1. \tag{11}$$

$$2 - 1/(2^n) = 2 - 1/(2^0) = 2 - 1 = 1. \tag{12}$$

Induction process:
suppose $\sum_{i=0}^{n} 1/(2^i)$=$2-(\frac{1}{2^n})$for n=0,1,2,3.....k;
at n=k+1,

$$\sum_{i=0}^{n} 1/(2^i) = \sum_{i=0}^{k+1} 1/(2^i) = 1/(2^{k+1}) + \sum_{i=0}^{k} 1/(2^i) \tag{13}$$

$$= 1/(2^{k+1}) + 2 - 1/(2^k) \tag{14}$$

$$= 2 - 1/(2(2^{k+1})) + 1/(2^{k+1}) \tag{15}$$

$$= 2 - 1/(2^{k+1}) \tag{16}$$

induction success theorem correct.

□

2.3 Injective relation

Theorem 8. *suppose function $h : \mathbb{Z} \to \mathbb{Z}$ is injective, then function $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x, y) = (h(x) - y, 3h(x) + 1)$ also is injective.*

Proof. Let (x,y) and (p,q) be elements of $\mathbb{Z}$ and suppose $f(x, y) = f(p, q)$, then

$$(h(x) - y, 3h(x) + 1) = (h(p) - q, 3h(p) + 1); \tag{17}$$

which means:

$$3h(x) + 1 = 3h(p) + 1 \to h(x) = h(p) \tag{18}$$

□

since $h : \mathbb{Z} \to \mathbb{Z}$ is injective function, $x = p$.
and

$$h(x) - y = h(p) - q \tag{19}$$

Therefore,

$$h(x) - y = h(p) - q \to -y = -q \to y = q \tag{20}$$

since $x = p$ and $y = q$, $(x, y) = (p, q)$
which means $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x, y) = (h(x) - y, 3h(x) + 1)$ is injective.

2.4 Uncountable

Theorem 9. *the cardinality of $\mathbb{P}$ (irrationals) is uncountable.*

Proof. lemma. $\mathbb{R}$ is uncountable
proof of lemma:
let [0,1) be the set of $(r_1, r_2, r_3 ..., r_m ...)$
$r_1 = 0.d_{11}d_{12}d_{13}...d_{1n}...$
$r_2 = 0.d_{21}d_{22}d_{23}...d_{2n}...$
$r_3 = 0.d_{31}d_{32}d_{33}...d_{3n}...$
.
$r_m = 0.d_{m1}d_{m2}d_{m3}...d_{mn}...$
Assume [0,1) is countable, then let's define a decimal sequence E.
E= $0.e_{11}e_{22}e_{33}...e_{kk}... \in [0, 1)$.
the d in the E have the property that
if $d_{11} = 1$, then $e_{11} = 2$.
if $d_{11} \neq 1$, then $e_{11} = 1$. then, E would disjoint with the any decimal sequence in [0,1).

so [0,1) is uncountable.
since [0,1) is a subset of $\mathbb{R}$, $\mathbb{R}$ is also uncountable.
we can define the $\mathbb{R}$ is the union of $\mathbb{Q}$ and $\mathbb{P}$.
since the $|\mathbb{Q}| = |\mathbb{N}|$, $\mathbb{Q}$ is countable.
since $\mathbb{R}$ is uncountable we proof by lemma, $\mathbb{P}$ would be uncountable.

□

2.5 Inheritance of Equivalence Relation

Theorem 10. *Let R and S be two equivalence relations on a set A. Define T and U as:*

$$xTy \iff xRy \cap xSy, \tag{21}$$

$$xUy \iff xRy \cup xSy, \tag{22}$$

The relations T would be equivalence relations but U may not.

Proof. to the both T and U, they own the property of reflexive and symmetric since R and S are equivalence relations.

however, when we consider the property of tansition between T and U, it would be different.

for the T, if xTy and yTz, then xRy, yRz,and xSy, ySz.

Since R and S are equivalence relations,

$$xRy, yRz \to xRz \tag{23}$$

$$xSy, ySz \to xSz \tag{24}$$

Then $xRz \cap xSz \to xTz$ T is reflexive, symmetric and transitive, would be a equivalence relation.

however, things happen with U would be different.

for the U, if xUy and yUz, then it means $xRy \cup xSy$ and $yRz \cup ySz$.

if we have xRy, yRz or xSy, ySz, we can obtain xRz or xSz, which U would be equivalence relations.

But, if we consist xUy with xRy, $x \not S y$ and yUz with $y \not R z$, ySz.

we would get

$$xRy, ySz \not\to xRz, xSz \tag{25}$$

then the property of transitive would be fail for U, which means U is not equivalence relations in some situation. □