ALGEBRA, HUNGERFORD

Remark.
- propositions (and their lemmas and corallaries) can be skipped if just following the main line of development
- see graphic of which chapters depend on which

1. INTRODUCTION: PREREQUISITES AND PRELIMINARIES

Remark. assume familiarity with fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

1.1. LOGIC.

Definition.
- statement has truth value true or false (not both)
- negation, and, or, implies, iff

1.2. SETS AND CLASSES.

Remark.
- will use Godel-Bernays axiomatic set theory
- will state just enough axioms to define cardinal numbers (§0.8) and category (§I.7)
- will write axioms using first-order predicate calculus
- axiomatic approach avoids paradoxes (statement and its negation are deducible) (which implies every statement is true)

Definition.
- class, membership, and equality are primative (undefined) notions
  standard model: class is collection of member elements, and can determine whether given object is a member
- equality properties:
  $\forall A, B, C, :\ A = A;\ A = B \Rightarrow B = A;\ (A = B \wedge B = C) \Rightarrow A = C;\ (A = B \wedge x \in A) \Rightarrow x \in B$
- axiom of extensionality $(x \in A \Leftrightarrow x \in B) \Rightarrow A = B$
  ie two classes with the same elements are equal
- set is any A st $\exists B$ st $A \in B$ ie any class member
  proper class is a class that is not a set
- axiom of formation $\forall$ statements $P(y)$ in first order predicate calculus with variable y, $\exists$ class A st $x \in A$ iff $P(y)$ is true
  ntn: $A = \{x | P(x)\}$

Example. Russel's paradox
define class $M = \{X | X \text{ is a set and } X \notin X\}$
M is a proper class, since if it were a set, then $M \in M$ or $M \notin M$
case $M \in M$: then $M \notin M$, contradiction
case $M \notin M$: then $M \in M$, contradiction
a parodox

Remark.
- next: construction of sets using unions, intersections, functions, relations, cartesian products, etc
- we assume sufficient axioms that these constructions performed on sets result in a set eg union of sets is a set
- the usual way to show that a class is a set is to construct it this way from sets

SUBCLASSES, SUBSETS, EMPTY SET

Definition.
- subclass $A \subset B$: $\forall x \in A, x \in A \Rightarrow x \in B$
- a subset is a subclass of a set
- empty set ("null set") $\emptyset$ is the set with no elements ie $\forall x, x \notin \emptyset$

Claim.
- $A = B \Leftrightarrow (A \subset B \text{ and } B \subset A)$
- $\forall B, \emptyset \subset B$

Proof.
- axiom of extensionality and properties of equality
- def of subclass, $x \in \emptyset$ is always false

POWER SET, INDEXED FAMILY OF SETS

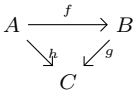
Definition.
- power axiom: powerset $P(A) = 2^A = \{\text{all subsets of } A\}$ (note: is indeed a set)
- a family of sets indexed by class I is $\{A_i | i \in I\}$
- union $\cup_{i \in I} A_i = \{x | x \in A_i \text{ for some } i \in I\}$
  intersection $\cap_{i \in I} A_i = \{x | x \in A_i \text{ for all } i \in I\}$
  ntn: for finite I, $A_1 \cup A_2 \cup ... \cup A_n$
  note: we have axioms that union and intersection of sets is a set, even if I not a set
- disjoint A, B means $A \cap B = \emptyset$
- the relative complement of A in B is the subclass $B - A = \{x | x \in B, x \notin A\}$
- the complement of A wrt some superset "universe" U is $A' = U - A$

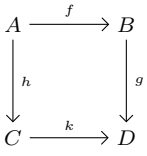
Claim.
- *(distribution)*
  $A \cap (\cup_{i \in I} B_i) = \cup_{i \in I} (A \cap B_i)$
  $A \cup (\cap_{i \in I} B_i) = \cap_{i \in I} (A \cup B_i)$
- *(deMorgan)*
  $(\cup_{i \in I} A_i)' = \cap_{i \in I} A_i'$
  $(\cap_{i \in I} A_i)' = \cup_{i \in I} A_i'$
- *(subclass, union, intersection)*
  $A \subset B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A$

1.3. FUNCTIONS.

Definition.
- a function ("map") f from domain $Dom(f) = A$ to codomain ("range") B, $f : A \to B$, assigns to each $a \in A$ exactly one $b \in B$
- the image ("value") of f at a is $f(a)$
  ntn: $a \mapsto f(a)$
- equal functions mean equal domain, range, and image of each element of domain
- the restriction of $f : A \to B$ to $S \subset A$ is function $f|_S : S \to B$ st $a \mapsto f(a)\ \forall a \in S$
- the identity function of A is function $1_A : A \to A$, $a \mapsto a \forall a \in A$
- the inclusion map of $S \subset A$ into A is $1_A|_S : S \to A$
- the composite of functions $f : A \to B$, $g : B \to C$ is function $g \circ f : A \to C$, $a \mapsto g(f(a))\ \forall a \in A$
  ntn: gf

Claim.
- *h(gf)=(hg)f where f, g, h have appropriate domains, codomains*
- *if $f : A \to B$, then $f \circ 1_A = f = 1_B \circ f$*

Definition.
- a diagram of functions is commutative means
  - case triangle: gf=h
    

  - case square: $kh = gf$
    

  - case diagram with many triangles and squares: each triangle and square is commutative
- the image of $S \subset A$ under $f : A \to B$ is the class $f(S) = Im(f) = \{b \in B | b = f(a) \text{ for some } a \in S\}$
- the inverse image of $T \subset B$ under $f : A \to B$ is class $f^{-1}(T) = \{a \in A | f(a) \in T\}$
  ntn: if T is singleton $\{b\}$, write $f^{-1}(b)$

Claim.
- *for $S \subset A$, $f^{-1}(f(S)) \supset S$*
  for $T \subset B$, $f(f^{-1}(T)) \subset T$
- *for any family of subsets of B*
  $f^{-1}(\cup_{i \in I} T_i) = \cup_{i \in I} f^{-1}(T_i)$
  $f^{-1}(\cap_{i \in I} T_i) = \cap_{i \in I} f^{-1}(T_i)$

Definition.
- injection ("1-1"): $\forall a, a' \in A\ a \neq a' \Rightarrow f(a) \neq f(a')$
- surjection ("onto"): $f(A) = B$ ie $\forall b \in B \exists a \in A$ st $f(a) = b$
- bijection ("1-1 correspondence"): both injection and surjection

Claim.
- *identity map is bijection*
- *Let $f : A \to B$, $g : B \to C$*
  f, g injective $\Rightarrow gf$ injective
  f, g surjective $\Rightarrow gf$ surjection
  gf surjection $\Rightarrow f$ injection and g surjection

Definition. Let $f : A \to B$, A nonempty
- left inverse of f is $g : B \to A$ st $gf = 1_A$
- right inverse of f is $h : B \to A$ st $fh = 1_B$
- two sided inverse is left and right inverse, may not exist

Theorem. *(3.1)*
i) injective $\Leftrightarrow$ exists left inverse
ii) surjective $\Leftrightarrow$ exists right inverse

Claim.
- *if f has left and right inverse g, h then $g = h = f^{-1}$ and is unique*
  pf: $g = g1_B = g(fh) = (gf)h = 1_A h = h$
- *$f : A \to B$ bijective $\Leftrightarrow$ f has 2-sided inverse*
- *if f bijective, f^{-1} is also a bijection*
  pf: its 2 sided inverse is f

1.4. RELATIONS AND PARTITIONS.

ORDERED PAIR, CARTESIAN PRODUCT, RELATION, GRAPH

Definition.
- axiom of pair formation: $\forall$ sets a, b, $\exists$ set $P = \{a, b\}$ st $x \in P$ iff $x = a$ or $x = b$; and if $a = b$, $P = \{a\}$
- ordered pair (a, b) is the set $\{\{a\}, \{a, b\}\}$ with first component a and second component b
  note: $(a, b) = (a', b')$ iff $a = a'$ and $b = b'$
- the cartesian product of classes A, B is class $A \times B = \{(a, b) | a \in A, b \in B\}$
  note: $A \times \emptyset = \emptyset = \emptyset \times B$
- a relation on $A \times B$ is a subclass R of $A \times B$
- a graph of function $f : A \to B$ is relation $R = \{(a, f(a)) | a \in A\}$
- special [single-value] property of relation $R \subseteq A \times B$ means every element of A is the first component of one and only one ordered pair in R

Claim. *if function then satisfies single-value property*
converse: if R satisfies single value property, then $\exists! f : A \to B$ whose graph is R (pf: define $f(a) = b$ where $(a, b) \in R$)

Remark. when convenient will define functions as relations satisfying single-value property
this allows proving "the image of a set under a function is a set"
this also allows defining: a function with empty domain vacously as empty set

EQUIVALENCE RELATIONS AND PARTITIONS

Definition.
- equivalence relation R on $A \times A$ means:
  (reflexive): $\forall a \in A$: $(a, a) \in R$
  (symmetric): $\forall a, b \in A$: $(a, b) \in R \Leftrightarrow (b, a) \in R$
  (transitive): $\forall a, b, c \in A$: $(a, b) \in R$, $(b, c) \in R \Rightarrow (a, c) \in R$
  ntn: aRb or $a \sim b$

- a is equivalent to b under equiv rel R means $(a,b) \in R$
- the equivalence class of $a \in A$ wrt equiv rel R is $\overline{a} = \{b \in B | b \sim a\}$
  ie class of elements equiv to a
- quotient class of A by equiv rel R is class A/R =all equiv classes of A

Claim.
- $\overline{a} \neq \emptyset$
- *let A a set*
  then $\cup_{a \in A} \overline{a} = A = \cup_{\overline{a} \in A/R} \overline{a}$
  pf: R is reflexive and $a \in \overline{a}$ $\forall a \in A$
- $\overline{a} = \overline{b} \Leftrightarrow a \sim b$
  pf: $(\Rightarrow)$ $\overline{a} = \overline{b} \Rightarrow a \in \overline{a} \Rightarrow a \in \overline{b} \Rightarrow a \sim b$
  $(\Leftarrow)$ *$a \sim b$ and $c \in \overline{a} \Rightarrow c \sim a, a \sim b \Rightarrow c \sim b \Rightarrow c \in \overline{b} \Rightarrow \overline{a} \subset \overline{b}$, and similarly for $\overline{b} \subset \overline{a} \Rightarrow \overline{a} = \overline{b}$*
- *for $a, b \in A$ either $\overline{a} \cap \overline{b} = \emptyset$ or $\overline{a} = \overline{b}$*
  pf: $\overline{a} \cap \overline{b} \neq \emptyset \Rightarrow \exists c \in \overline{a} \cap \overline{b} \Rightarrow c \sim a, c \sim b \Rightarrow a \sim c, c \sim b \Rightarrow a \sim b \Rightarrow \overline{a} = \overline{b}$

Definition. a partition of nonempty class A is family $\{A_i | i \in I\}$ of subsets of A st $A_i \neq \emptyset \forall i \in I$, $\cup_{i \in I} A_i = A$, and $A_i \cap A_j = \emptyset \forall i \neq j \in I$

Theorem. *(4.1)*
Let A nonempty set
$R \mapsto A/R$ defines a bijection of set $E(A)$ =all equiv rels of A onto the set $R(A)$ =all partitions of A

1.5. PRODUCTS.

Remark. this section only deals with sets, no proper classes

Claim. *$\exists$ a bijection between $A_1 \times A_2$ and the set of all functions $f : \{1,2\} \to A_1 \cup A_2$ st $f(1) \in A_1$ and $f(2) \in A_2$*
(so can characterize $A_1 \times A_2$ with functions)

Proof. Let $(a_1, a_2) \in A_1 \times A_2$
define function $f : \{1,2\} \to A_1 \cup A_2$ by $f(a) = a_1, f(2) = a_2$
conversely, let $f : \{1,2\} \to A_1 \cup A_2$ st $f(1) \in A_1$, $f(2) \in A_2$
this function corresponds to $(f(1), f(2)) = (a_1, a_2) \in A_1 \times A_2$

Remark. next, generalize above to arbitrary size

Definition. Let family of sets $\{A_i | i \in I\}$
the cartesian product of sets A_i is the set of all $f : I \to \cup_{i \in I} A_i$ st $f(i) \in A_i \forall i \in I$
ntn: $\prod_{i \in I} A_i$
ntn: for finite $I = \{1, 2, ..., n\}$, $A_1 \times A_2 \times ... \times A_n$
ntn: $f \in \prod_{i \in I} A_i$ denoted $\{a_i\}_{i \in I}$ or $\{a_i\}$ where $f(i) = a_i \forall i \in I$
note: if some $A_j = \emptyset$, then $\prod_{i \in I} A_i$ is empty since cant have $f(j) \in A_j$

Claim. *Let $\{A_i | i \in I\}$ and $\{B_i | i \in I\}$ families of sets*
$B_i \subset A_i \forall i \Rightarrow \prod_{i \in I} B_i \subset \prod_{i \in I} A_i$

Proof. each function $I \mapsto \prod_{i \in I} B_i$ is also a function $I \mapsto \prod_{i \in I} A_i$

UNIVERSAL MAPPING PROPERTY

Definition. the (cononical) projection of functions in $\prod_{i \in I} A_i$ onto its $k(\in I)$th component ("factor") is map $\pi_k : \prod_{i \in I} A_i \to A_k$, $f \mapsto f(k)$ ie $\{a_i\} \mapsto a_k$

Claim. *if every A_i is nonempty, then each π_k is surjective*
pf: exercise 7.6

Theorem. *(5.1)*
Let $\{A_i | i \in I\}$ family of sets
then $\exists$ set D and a family of maps $\{\pi_i : D \to A_i | i \in I\}$ st
$\forall$ set C and family of maps $\{\phi_i : i \to A_i | i \in I\}$ $\exists! \phi : C \to D$ st $\pi_i \phi = \phi_i \forall i \in I$
furthermore D is unique up to bijection (ie if exists $D', \{\pi_i'\}$ with same property as $D, \{\pi_i\}$ then $\exists$ bijection $D \mapsto D'$)

Remark.
- above thm does not mention elements, only sets and maps
- this thm says that product $\prod_i A_i$ is characterized by a certain universal mapping property
- will discuss further when get to categories and functors

1.6. THE INTEGERS.

Remark.
- will not give axiomatic development of the integers
- assume know sets $\mathbb{Z}$, $\mathbb{N} = \{0, 1, 2, ...\}$, $\mathbb{N}^* = \{1, 2, ...\}$ and properties of addition, multiplication, and order
  (associative) $(a+b)+c = a+(b+c)$, $(ab)c = a(bc)$
  (commutative) $a + b = b + a$, $ab = ba$
  (distributive) $a(b+c) = ab+ac$, $(a+b)c = ac+bc$
  (identities) $a + 0 = a$, $a1 = a$
  (additive inverse) $\forall a \in \mathbb{Z} \exists! -a \in \mathbb{Z}$ st $a + (-a = 0)$; ntn $a - a$
  (order) $ab = 0 \Leftrightarrow a = 0 \vee b = 0$; $a < b \Rightarrow a + c < b + c \forall c \in \mathbb{Z}$; $a < b \Rightarrow ad < bd \forall d \in \mathbb{N}^*$
  ntn: $a > b$ means $b < a$; $a \leq b$ iff $a < b \vee a = b$; $|a| = a$ if $a \geq 0$ and $-a$ if $a < 0$

INDUCTION AND RECURSION

Definition. axiom law of well ordering: every nonempty subset S of $\mathbb{N}$ contains a least element ($b \in S$ st $b \leq c \; \forall c \in S$)
in particular, 0 is least element of $\mathbb{N}$

Theorem. *(6.1) (principle of mathematical induction)*
if $S \subset \mathbb{N}$ st $0 \in S$ and either
1) $a \in S \Rightarrow n + 1 \in S \; \forall n \in \mathbb{N}$ or
2) $m \in S \; \forall 0 \leq m < n \Rightarrow n \in S \; \forall n \in \mathbb{N}$
then $S = \mathbb{N}$
note: this extends to $0, \mathbb{N}$ replaced by $c, M_c = \{x \in \mathbb{Z} | x \geq c\}$

Theorem. *6.2 (Recursion thm)*
if S a set, $a \in S$, $\forall n \in \mathbb{N}$, $f_n : S \to S$
then $\exists! \phi : \mathbb{N} \to S$ st $\phi(0) = a$ and $\phi(n+1) = f_n(\phi(n)) \; \forall n \in \mathbb{N}$
note: will use this in eg thm 8.8, thm III.3.7, to show recursive or inductive defs are valid

Definition. a sequence in A is a function $\mathbb{N} \to A$ (or $\mathbb{N}^* \to A$)
ntn: $\{a_i\}_{i \in \mathbb{N}} = \{a_i\} = \{a_0, a_1, a_2, ...\}$

DIVISION; PRIMES; FUND THM ARITHMETIC

Theorem. *(6.3) (Division algorithm)*
if $a, b \in \mathbb{Z}$ and $a \neq 0$, then $\exists! q, r$ st $b = aq + r$ and $0 \leq r < |a|$

Definition. integer $a \neq 0$ divides b, $a \mid b$, means $\exists k \in \mathbb{Z}$ st $ak = b$
ntn: otherwise, $a \nmid b$

Definition. (6.4)
the greatest common divisor of integers $a_1, a_2, ..., a_n$ is positive integer c st (1) $c \mid a_i$ $1 \leq i \leq n$ and (2) $d \in \mathbb{Z}$ and $d \mid a_i$ for $1 \leq i \leq n \Rightarrow d \mid c$
ntn: $c = (a_1, a_2, ..., a_n)$

Theorem. *(6.5)*
if $a_1, a_2, ..., a_n \in \mathbb{Z}$ not all 0, then $(a_1, a_2, ..., a_n)$ exists
furthermore, $\exists k_1, c_2, ..., k_n$ st $(a_1, a_2, ..., a_n) = k_1 a_1 + k_2 a_2 + ... + a_n k_n$

Definition.
- relatively prime integers $a_1, a_2, ..., a_n$ means $(a_1, a_2, ..., a_n) = 1$
- prime integer $p > 1$ means its only divisors are ± 1 and $\pm p$

Claim. *if p prime and $a \in \mathbb{Z}$, then either*
case $p \mid a$: $(a, p) = p$
case $p \nmid a$: $(a, p) = 1$

Theorem.
- *if a, b are relatively prime and $a \mid bc$ then $a \mid c$*
- *if p is prime and $p \mid a_1 a_2 ... a_n$ the $p \mid a_i$ for some i*

Theorem. *(fundamental thm of algebra)*
any integer $n > 1$ can be written $n = p_1^{t_1} p_2^{t_2} ... p_k^{t_k}$ where $p_1 < p_2 < ... < p_k$ and $t_i > 0 \; \forall i$

MODULO/CONGRUENCE

Definition. let $m > 0$ integer, $a, b \in \mathbb{Z}$. a is congruent to b modulo m means $m \mid (b - a)$
ntn: $a \equiv b \mod m$

Theorem. *(6.8)*
let $m > 0$ integer, $a, b, c, d \in \mathbb{Z}$. then
i) congruence modulo m is an equiv rel on $\mathbb{Z}$, has m equiv classes
ii) $a \equiv b \mod m$ and $c \equiv d \mod m \Rightarrow a + c \equiv b + d \mod m$ and $ac \equiv bd \mod m$
iii) if $ab \equiv ac \mod m$ and a, m are relatively prime $\Rightarrow b \equiv c \mod m$

1.7. THE AXIOM OF CHOICE, ORDER, AND ZORN'S LEMMA.

Remark.
- this section only deals with sets, no proper classes
- relationship between the three topics of this section:
  AoC $\Leftrightarrow$ Zorn's Lemma $\Leftrightarrow$ well ordering principle

Definition. axiom of choice The product of a famuly of nonempty sets indexed by a nonempty set is nonempty
note: another version in exercises

ORDER

Definition.
- a partially ordered set is a nonempty set A together with a relation R on $A \times A$ (called a partial ordering of A) which is reflexive, transitive, and antisymmetric ($(a, b) \in R, (b, a) \in R \Rightarrow a = b$)
  ntn: $a \leq b$ means $(a, b) \in R$
  ntn: $a < b$ means $a \leq b$ and $a \neq b$
- comparable elements $a, b \in A$ (wrt partial ordering) means $a \leq b$ or $b \leq a$
- linear ordering ("total ordering", "simple ordering") is partial ordering st any two elements are comparable

Example. let A be power set of $\{1, 2, 3, 4, 5\}$
define order relation on subsets of A: $C \leq D$ iff $C \subset D$
then A is partially ordered, but not linearly ordered (eg $\{1, 2\}$ and $\{3, 4\}$ not comparable)

ZORN'S LEMMA

Definition. Let A nonempty, partially ordered by $\leq$
- maximal element of $(A, \leq)$ is $a \in A$ st for every $c \in A$ which is comparable to a, $c \leq a$ ie $a \leq c \Rightarrow a = c$
  note: need not be unique or even exist (eg for $\mathbb{Z}$ with usual ordering)
- an upper bound of a nonempty subset B of A is an element $d \in A$ st $b \leq d$ for every $b \in B$
- a chain in A is a subset B that is linearly ordered by $\leq$

- Zorn's lemma: if every chain in A has an upper bound in A then A contains a maximal element (will use this powerful tool)

WELL ORDERING PRINCIPLE

Definition.
- a well ordered set A is total ordered and every nonempty subset B has a least element $c \in B$ ($c \leq b \; \forall b \in B$)
- well ordering principle: nonempty set $A \Rightarrow \exists$ linear ordering $\leq$ of A st $(A, \leq)$ is well ordered
- the immediate predecessor of an element a in a well-ordering is c st a is the least element of $\{x | c < x\}$

Claim. *well ordered $\Rightarrow$ linearly ordered*
well ordered $\not\Leftarrow$ linearly ordered

Proof. $\forall a.b \in A$ $\{a, b\}$ must have a least element ie $a \leq b$ or $b \leq a$

Example.
- $\mathbb{N}$ is well ordered, see previous section
- $\mathbb{Z}$ with usual ordering is linearly ordered but not well ordered, eg negatives have no least element but can choose another ordering under which $\mathbb{Z}$ is well ordered...
- i) $0, 1, -1, 2, -2, 3, -3, ..., n, -n, ...$
  every nonzero element has an immediate predecessor
  no maximal elements
  ii) $0, 1, 3, 5, 7, ..., 2, 4, 6, 8, ..., -1, -2, -3, -4, ...$
  2 and -1 have no immediate predecessor
  no maximal elements
  iii) $0, 3, 4, 5, 6, ..., -1, -2, -3, -4, ..., 1, 2$
  -1 and 1 have no immediate predecessor
  2 is maximal element
  0 is least element in all three

Remark. well-ordering principle allows extending mathematical induction for positive integers (6.1) to any well ordered set

Theorem. *(principle of transfinite induction)*
B is a subset of well ordered set $(A, \leq)$ st $\forall a \in A$ $(\{c \in A | c < a\} \subset B \Rightarrow a \in B)$
$\Rightarrow B = A$

1.8. CARDINAL NUMBERS.

Remark. will often use this section up to 8.5
will occasionally use stuff from thm 8.5 to end (see book for specific thms, lems) and may be omitted-for now

Definition.
- equipollent sets A, B means $\exists$ bijection $A \to B$
  ntn: $A \sim B$
- A has precisely n elements means equipollent to $I_n = \{1, 2, ..., n\}$ (with $I_0 = \emptyset$)
- finite set A means $A \sim I_n$ for some unique $n \geq 0$
  infinite otherwise

Theorem. *(8.1)*
Equipollence is an equivalence relation on the class S of all sets

Definition. (8.2)
- the cardinal number of set A, $|A|$, is the equivalence class of A under the equivalence relation of equipollence
  ntn: lower case greek letters eg α, β, γ
  note: we defined cardinal number as a proper class, but elsewhere it is usually defined as a set, but many results are same both defs, since they are just statements about the equipollence of sets
- finite (infinte) cardinal number means finite (infinite) set
  ntn: for finite, identify integer $n > 0$ with $|I_n|$ and write $|I_n| = n$
- ntn: $\aleph_0 = |\mathbb{N}|$
- denumerable set A means $|A| = \aleph_0$

Claim.
- *i) every set has a unique cardinal number*
  ii) two sets have the same cardinal number iff they are equipollent ie $|A| = |B| \Leftrightarrow A \sim B$
  iii) the cardinal number of a finite set is the number of elments in the set
  $\mathbb{Z}, \mathbb{Q}$ are denumerable, $\mathbb{R}$ is not

Definition. (8.3) (cardinal arithmetic)
Sum of cardinal numbers $\alpha = |A|$ and $\beta = |B|$ is $\alpha + \beta = |\alpha \cup \beta|$ where A, B disjiont sets
product is $\alpha\beta = |A \times \beta|$

Claim.
- *$\forall$ cardinal numbers α $\exists A$ st $\alpha = |A|$*
  also, for addition, disjoint sets always exist
- *the sum and product are indep of choice of sets*
- *addition and multiplication of cardinals are associative, commutative, and distributive*
- *addition and multiplication of finite cardinals agree with regualar addition of nonnegative integers with which they are identified*

Definition. (8.4)
Let sets $A.B$ and $\alpha = |A|, \beta = |B|$
α is less than or equal to β, $\alpha \leq \beta$ or $\beta \geq \alpha$, means A is equipollent with a subset of B (ie exists injection $A \to B$)
α is strictly less than β, $\alpha < \beta$ or $\beta > \alpha$, means $\alpha \leq \beta$ and $\alpha \neq \beta$

Claim. *def of $\leq$ does not depend on choice of A and B*
for finite cardinals, $\leq$ agrees with usual ordering

Theorem. *(8.5)*
Let set A. $|A| < |P(A)|$ where P is powerset

Corollary. *there is no largest cardinal number*

Claim. $\aleph_0 = |\mathbb{N}| < |P(\mathbb{N})| = |\mathbb{R}|$

Definition. continuum hypothesis (CH): there is no β st $|\mathbb{N}| < \beta < |\mathbb{R}|$
rmk: CH is indep of AoC and the axioms of set theory

Theorem. *(8.6) (Schroeder-Bernsteim)*
A, B sets st $|A| \leq |B|$ and $|B| \leq |A|$
$\Rightarrow |A| = |B|$

Theorem. *(8.7)*
- *the class of all cardinal numbers is linearly ordered by $\leq$*
- *(trichotomy) let cardinals α, β. Exactly one of these holds: $\alpha < \beta; \alpha = \beta; \beta < \alpha$*

Remark. pf of 8.7 defined partially ordered family of functions which were ordered by extension
note: this pf was typical use of zorn's lemma

Theorem. *(8.8)*
every infinite set has a denumerable subset
in particular, $\aleph_0 \leq \alpha$ for every infinite cardinal α

Lemma. *(8.9)*
if A infinte set and F a finite set, then $|A \cup F| = |A|$
in particular $\alpha + n = \alpha$ for α infinite and n finite

Theorem. *(8.10)*
if α, β cardinals st $\beta \leq \alpha$ and α infinite
then $\alpha + \beta = \alpha$

Theorem. *(8.11)*
if α, β cardinals st $0 \neq \beta \leq \alpha$ and α infinite
then $\alpha\beta = \alpha$
in particular, $\alpha\aleph_0 = \alpha$ and if β finite, $\aleph_0\beta = \aleph_0$

Theorem. *Let set A and for each integer $n \geq 1$*
ntn $A^n = A \times A \times ... \times A$ (n factors)
i) A finite then $|A^n| = |A|^n$
A infinite then $|A^n| = |A|$
ii) $|\cup_{n \in \mathbb{N}^*} A^n| = \aleph_0 |A|$

Corollary. *A infinte set and $F(A)$ is the set of all finite subsets*
then $|F(A)| = |A|$