PREFACE

Remark. will answer:
- What is mathematical proof?
- How can proofs be justified?
- Are there limits to provability?
- To what extent can machines carry out mathematical proof?

Remark. results of this book:
- Godel's completeness thm - the consequence relation coincides with formal provability: by means of a calculus consisting of simple formal inference rules, one can obtain all consequences of a given axiom system (and in particular, imitate all of mathematics)
- model theory will help us analyze expressive power of the first-order language, and certain deficiencies.
  deficiencies: 1st order logic does not allow formulating an adequate axiom system for arithmetic or analysis
  power: this deficiency can be overcome in the framework of first order logic by developing math in set-theoretic terms (we will study set theory and its subtle relation to logic)
- Godel's incompleteness thm (and related thms like Trahtenbrot's) - exemplify limits of machine-oriented proof methods (will study computability theory using a register machine as a computer model)
- Herbrand's thm - starting point for theoretical fundamentals of logic programming, uses proof of Godel's completeness thm
- second order language and infinitary languages - logic systems with more expressive power than first order logic; will see that they lack central facts valid in first order languages (Lindstrom's thm - there is no logical system that extends first-order logic and shares all of its advantages)
- this book is translated from German

1. INTRODUCTION

Remark. Relation between mathematical logic and math:
1) Motivation and goals: Mathematical logic arose in searching for foundations of Math
   – Frege based Math on logic and set theory
   – Russel tried to eliminate contradictions in Frege's system
   – Hilbert's program: "the generally accepted methods of math do not lead to a contradiction"
2) Methods: definitions and arguments
3) Applications: mathematical logic has applications in algebra, topology, and theoretical computer science

Remark. Relation between traditional logic and mathematical logic:
- Both study objects such as deductions and proofs but math has specific methods and subjects.
- Is mathematical logic caught in vicious cycle due to limited methods and subjects? See ch 7.

1.1. AN EXAMPLE FROM GROUP THEORY.

Remark. In this and next section, will illustrate two mathematical proofs. Then will raise questions motivating rest of book

Definition.
- Axioms of group theory
  Let set G; $\circ : G \times G \to G$; $e, x, y, z \in G$
  (G1) $\forall x, y, z,\ (x \circ y) \circ z = x \circ (y \circ z)$
  (G2) $\forall x,\ x \circ e = x$
  (G3) $\forall x \exists y$ st $x \circ y = e$
- group is structure $(G, \circ^G, e^G)$ satisfying $G1, G2, G3$

Example. additive group of the reals $(\mathbb{R}, +, 0)$
not group: $(\mathbb{R}, \cdot, 1)$ since (G3) violated for $x = 0$

Theorem. *1.1 (existence of left inverse)*
for every x there is y st $y \circ x = e$

Proof. Choose x.
exists y st $x \circ y = e$ by (G3)
for this y, exists z st $y \circ z = e$ by (G3)
so $y \circ x = (y \circ x) \circ e$ by (G2)
$= (y \circ x) \circ (y \circ z)$ by plugging second line
$= y \circ (e \circ z)$ by (G1),(G1), then plugging first line
$= y \circ z$ by (G1) then (G2)
$= e$ by plugging second line

Remark. so every structure for which $G1, G2, G3$ are satisfied, there exists a left inverse
ie existence of left inverse *follows from* (*is a consequence of*) axioms of group theory

1.2. AN EXAMPLE FROM THE THEORY OF EQUIVALENCE RELATIONS.

Definition.
- Let set A; binary relation $R^A \subseteq A \times A$ (written R if no ambiguity); $x, y, z \in A$
  (E1) $\forall x,\ xRx$ (R is said "is equivalent to")
  (E2) $\forall x, y,\ xRy \Rightarrow yRx$
  (E3) $\forall x, y, z,\ xRy, yRz \Rightarrow xRz$
- equivalence structure (A, R^A), where R^A is called equivalence relation, satisfies $E1, E2, E3$

Example. $(\mathbb{Z}, R_5)$ where $R_5 = \{(a, b) | a, b \in \mathbb{Z}, b - a$ is divisible by $5\}$

Theorem. *2.1*
If $\exists u$ st xRu and yRu
then $\forall z,\ xRz \Leftrightarrow yRz$

Proof. Assume hypothesis.
(E2),(E3) xRy and yRx
assume $\exists z$ st xRz (or yRz)
(E2),(E3) $xRz \Rightarrow yRz$ ($yRz \Rightarrow xRz$)

Remark. so any structure that satisfies E1,E2,E3 also satisfies thm 2.1 ie thm follows from axioms.

1.3. A PRELIMINARY ANALYSIS.

Remark. both proofs assume set of propositions Φ called axioms to prove a proposition ψ

Definition. informally:
- everyday language proposition corresponds to formal formula (finite symbol string built up in a standard way eg $\forall x \forall y \forall z((x \equiv y \wedge y \equiv z \to x \equiv z))$) from an alphabet (eg quantifiers $\exists, \forall$ and connectives $\wedge, \to, \equiv$, and variables x, y, z) of formal language L (which is not as expressive as every-day language, but is, in principal, sufficient for all of math)
- proposition ψ follows from ("is a consequence relation of") propositions Φ means ψ holds for every structure satisfying Φ
- proof of proposition ψ from Φ is a series of inferences from Φ and already proved propositions which ends with ψ
  more formally, a sequence of L-formulas, each obtained using inference rules, which ends in ψ

Remark.
- ch 2: definition of formal language L
- ch 3: consequence relation ("follows from") - (ψ is a consequence of Φ) $\Leftrightarrow$ (ψ holds in every structure where all formulas of Φ hold)
- ch 4: finite system G of rules corresponding to math inference steps. These inferences can be represented as operations on L-formulas
- ch 5: Is every ψ which follows from Φ also provable from Φ?
  Yes, $\exists$ a proof (Godel's Completeness thm)
  this is a bridge between notion of proof, which is formal, and notion of consequence, which refers to the meaning of structures

Remark. mathematical proofs can be imitated by formal proofs in L

1.4. PREVIEW.

Remark.
- ch 6 - algebraic investigations, using ch 5's connection between proof and consequence
- ch 7 and 10 - investigation of consistency of mathematics; justification of rules of inference used in math
- ch 10 - scope and limitation of machine-oriented methods
- ch 11 - application of logic: interpret L-formulas as operations eg $\phi \Rightarrow \psi$ is operation from ϕ to ψ; logic programming - the starting point of certain computer language in artificial intelligence
- ch 9 - L is first-order language means L-formulas have first-order variables (refer to elements of domain of structure), not second order variables (refer to subsets eg for all subsets)
- ch 13 - L is a "best possible" language - more expressive languages lack useful properties

2. SYNTAX OF FORMAL LANGUAGES

this chapter: introduce the first order languages

2.1. ALPHABETS.

Definition.
- alphabet A is nonempty set of symbols
- string ("word") over A is finite sequence of symbols from A
- A^* denotes the set of all strings over A
- length of string $\zeta \in A^*$ is number of symbols, counting repetitions
- empty string $\square \in A^*$ has zero length

Example.
- alphabets:
  $A_1 = \{0, 1, 2, \ldots, 9\}$
  $A_2 = \{a, b, c, \ldots, z\}$
  $A_3 = \{\circ, \int, a, d, x, f,), (\}$
  $A_4 = \{c_0, c_1, c_2, \ldots\}$
- strings over A_2 are $softly$ and $xdbxaz$
  strings over A_3 are $\int f(x)dx$, $x \circ \int \int a$

Remark.
- will only consider alphabets st any string can be read in exactly one way
  eg $A_1, \ldots, A_4$ satisfy this. but $A_5 = \{|, ||\}$ does not since $|||$ can be read in three different ways
- next, want to know the number of strings over a given alphabet

Definition.
- countable set M means not finite and $\exists$ surjection $\alpha : \mathbb{N} \to M$ ie can represent $M = \{\alpha(n) | n \in \mathbb{N}\}$
- at most countable set M means finite or ctble

Lemma. *(1.1)*
Let nonempty set M
The following are equivalent:
a) M is at most ctble
b) $\exists$ surjective map $\alpha : \mathbb{N} \to M$
c) $\exists$ injective map $\beta : M \to \mathbb{N}$

Proof.
(a$\Rightarrow$ b)
if ctble M, then true by def
if finite $M = \{a_0, a_1, ..., a_n\}$ then define surjection $\alpha : \mathbb{N} \to M$, $\alpha(i) := a_i$ if $0 \le i \le n$, and a_0 o.w.
(b$\Rightarrow$ c)
Let surjection $\alpha : \mathbb{N} \to M$.
define injective map $\beta : M \to \mathbb{N}$, $\beta(a) :=$ least i st $\alpha(i) = a$
(c$\Rightarrow$ a)
let injective map $\beta : M \to \mathbb{N}$
if M finite, done.
if M not finite, must show M is ctble
define surjective map $\alpha : \mathbb{N} \to M$ inductively:

$\alpha(0) = a \in M$ with the smallest image under β in M
$\alpha(n+1) = a \in M$ with the smallest image under β greater than $\beta(\alpha(0)), ..., \beta(\alpha(n))$
α is defined for all $n \in \mathbb{N}$ since the images under β are not bdd in $\mathbb{N}$
every $a \in M$ belongs to the range of α

Remark.
- it is circular to use proofs before making precise what a proof is. Will address this in ch 7
- using lem 1.1, can show
  - every subset of an at most ctble set is at most ctble
  - if M_1, M_2 are at most ctble, then so is $M_1 \cup M_2$
- $\mathbb{R}$ is neither finite nor ctble, it is unctble (ex 1.3)

Remark. will later see
- finite alphabets suffice for representing mathematical statements
- symbols may be chosen as "concrete" objects ie included on a keyboard
- can often improve transparency of an argument by using ctble alphabet like A_4 and we shall do this frequently
- sometimes useful to consider unctble alphabets eg $\{c_r | r \in \mathbb{R}\}$
  justified in §7.4

Lemma. *(1.2)*
if A is at most ctble alphabet
then A^* is ctble

Proof. Let prime numbers $p_0 = 1, p_1 = 3, p_2 = 5, ...$
Let finite $A = \{a_0, ..., a_n\}$ (or ctble $A = \{a_0, a_1, ...\}$) where elements of A are pairwise distinct
define map $\beta : A^* \to \mathbb{N}$, $\beta(\square) := 1$, $\beta(a_{i_0}...a_{i_n}) := p_0^{i_0+1} \cdot ... \cdot p_n^{i_n+1}$
clearly β is injective
thus A^* is at most ctble (cf 1.1c)
A^* cannot be finite since $a_0, a_0a_0, a_0a_0a_0, ...$ are all in A^*
hence A^* is ctble

2.2. THE ALPHABET OF A FIRST ORDER LANGUAGE.

Remark. need to construct formal languages in which we can formulate axioms, theorems, and proofs, eg those in ch1 about groups and equivalence relations

Definition.
- the alphabet of a first-order language contains the following symbols, all distinct
  a) variables $v_0, v_1, v_2, \cdots$
  b) connectives $\neg, \wedge, \vee, \to, \leftrightarrow$ (not, and, or, if... then..., iff)
  c) quantifiers $\forall, \exists$ (for all, there exists)
  d) equality relation $\equiv$
  e) auxiliary symbols), ((parentheses)
  f1) $\forall n \geq 1$, a (possibly empty) set of n-ary relation symbols $R_0^n, R_1^n, R_2^n, \cdots$
  f2) $\forall n \geq 1$, a (possibly empty) set of n-ary function symbols $f_0^n, f_1^n, f_2^n, \cdots$
  f3) a (possibly empty) set of constants $c_1, c_2, c_3, \cdots$
- symbol set A is elements from (a) through (e)
  symbol set S is elements in (f)
- alphabet of a first order language is $A_S = A \cup S$

Remark. S determines a first order language

Example.
- group theory $S_{gr} := \{\circ, e\}$
- equivalence relation theory $S_{eq} := \{R\}$
- ordered group theory $S_{ogr} := \{\circ, e, R\}$ where R is the ordering relation
- $S_\infty := \{c_0, c_1, c_2, \cdots, R_0^n, R_1^n, R_2^n, \cdots, f_0^n, f_1^n, f_2^n, \cdots\}$

Remark. notation henceforth:
P, Q, R are relation symbols
f, g, h are function symbols
x, y, z are variables

2.3. TERMS AND FORMULAS OF FIRST ORDER LANGUAGES.

Remark. want to define specific types of strings over A_S using a system of *instructions* ("rules") called a *calculus*

Definition.
- S-term is a string in A_S^* which can be obtained by finitely many applications of the following rules
  (T1) every variable is a S-term
  (T2) every constant in S is a S-term
  (T3) if strings $t_1, \cdots, t_n$ are S-terms and f is an n-ary function symbol in S, then $ft_1 \cdots t_n$ is also an S-term
- T^S is the set of S-terms

Remark. can determine whether string is S-term by applying rules of the calculus of terms

Example.
- gv_0fgv_4c is a $\{f, g, c\}$-term where f is unary func, g is binary func
  Pf: *derive* in the calculus of terms
  1. c T2
  2. v_0 T1
  3. v_4 T1
  4. gv_4c T3 to 3,1 using g
  5. fgv_4c T3 to 4 using f
  6. gv_0fgv_4c T3 to 2,5 using g
- $\circ x \circ ey$ is a S_{gr}-term
  1. x T1
  2. y T1
  3. e T2
  4. $\circ ey$ T3 on 2,3 using $\circ$
  5. $\circ x \circ ey$ T3 on 1,4 using $\circ$
  notation: will use eg $x \circ (e \circ y)$ for easier reading

Definition.
- S-formula is a string in A_S^* which is obtained by finitely many applications of the following rules
  (F1) if t_1 and t_2 are S-terms, then equation (equality symbol with term on each side) $t_1 \equiv t_2$ is an S-formula
  (F2) if $t_1, \cdots, t_n$ are S-terms and R is a n-ary relation symbol in S, then $Rt_1 \dots t_n$ is an S-formula
  (F3) if ϕ is an S-formula, then $\neg\phi$ (negation of ϕ) is also an S-formula
  (F4) if ϕ and ψ are S-formulas, then conjunction $(\phi \wedge \psi)$ ("conjunction of ϕ and ψ"), disjunction $(\phi \vee \psi)$, implication $(\phi \to \psi)$, and $(\phi \leftrightarrow \psi)$ are also S-formulas
  (F5) if ϕ is an S-formula and x is a variable, then $\forall x\psi$ and $\exists x\psi$ are also S-formulas
- atomic S-formulas are derived using (F1) and (F2) ie not formed by combining other S-formulas
- L^S denotes the set of S-formulas and is called "the first-order language associated with symbol set S" and "the language of first-order predicate calculus associated with S"

Example. consider S_{gr}
example formulas: $e \equiv e, e \circ v_1 \equiv v_1, \exists v_2(e \equiv e \wedge v_1 \equiv v_2)$
not formulas: $\equiv \wedge e, e \vee e$

Remark.
- notation:
  -can drop "S" from S-term and S-formula
  -$t, t_0, t_1, \cdots$ denote terms
  -$\phi, \psi, \cdots$ denote formulas
- can express axioms as formulas
- can verify whether a string is a formula by giving derivation in the calculus of S-formulas, similar to that of S-terms

Example.
- axioms of equiv relations, $S_{eq} = \{R\}$, are formulas
  (E1) $\forall v_0 Rv_0v_0$
  (E2) $\forall v_0 \forall v_1 (Rv_0v_1 \to Rv_1v_0)$
  (E3) $\forall v_0 \forall v_1 \forall v_2 ((Rv_0v_1 \wedge Rv_1v_2) \to Rv_0v_2)$
- (E1) is a formula:
  1. Rv_0v_0 (F2)
  2. $\forall v_0 Rv_0v_0$ (F5) applied to 1 using $\forall v_0$
- (E2) is a formula
  1. Rv_0v_1 (F2)
  2. Rv_1v_0 (F2)
  ⋮

Remark. despite its rigor, the calculus of formulas has liberal aspects.
eg consider $S = \{P, Q, f, g\}$ where f unary, g binary, P unary, Q ternary.
1) can quantify over a variable which does not occur in the formula in question eg $\forall y(Pz \to Qxxz)$
2) can join two identical formulas by means of a conjunction eg $(Pgxfy \to \exists x(x \equiv x \wedge x \equiv x))$
3) can quantify several times over the same variable eg $\forall z \forall z \exists z Qxyz$

Remark. notation:
- Rv_0v_1 can be written v_0Rv_1 (and sometimes $v_0 < v_1$)
- will omit nonessential parentheses
  - associate conjunctions and disjunctions to left eg $\phi \wedge \psi \wedge \xi$ means $((\phi \wedge \psi) \wedge \xi)$
  - $\wedge, \vee$ bind stronger than $\to$ eg $\forall x(\phi \wedge \psi \to \xi)$ means $\forall x((\phi \wedge \psi) \wedge \xi)$
- but need full formulas to have a precise notion of mathematical statement in our analysis of the notion of proof
  analogy: computer programers need precise implementation but can have non-precise discussion
- using $\equiv$ allows us to write statements like $\phi =$ "ϕ is the formula $x \equiv y$"

Lemma. *3.3*
if S is at most ctble
then T^S and L^S are ctble
(this will be useful later)

Proof. Let S at most ctble
then so is A_S and by lem 1.2 the set A_S^*
then so are T^S and L^S which are subsets of A_S^*
T^S and L^S are infinite since T^S contains variables $v_0, v_1, v_2, \cdots$ and L^S contains formulas $v_0 \equiv v_0$, $v_1 \equiv v_1$, $v_2 \equiv v_2$,... even if $S = \emptyset$

Definition.
- object language is the object of our investigation
- metalanguage is the language in which the investigation is carried out

Example.
- for us, L^S is object language and English is metalanguage
- in linguistics, english is the object language
- in certain set theoretic investigations (§7.4.3), first order languages are metalanguage

Remark. Frege developed the first comprehensive formal language, but it was complicated
Peano introduced modern formal languages

2.4. INDUCTION IN THE CALCULUS OF TERMS AND IN THE CALCULUS OF FORMULAS.

Definition. let S and let set of strings $Z \subset A_S^*$
calculus $\mathfrak{C}$ is a set of rules, schematically $\frac{\zeta_1, \cdots, \zeta_n}{\zeta}$, where strings $\zeta_1, \cdots, \zeta_n \in Z$ and ζ another string, that say
1) certain strings ζ belong to Z premise-free ie $n = 0$ (eg T1,T2,F1,F2)

2) if $\zeta_1, \cdots, \zeta_n \in Z$ then $\zeta \in Z$ ie permit passage from $\zeta_1, \cdots, \zeta_n$ to ζ

Example. rules for calculus of terms:
(T1) $\frac{}{x}$
(T2) $\frac{}{c}$ if $c \in S$
(T3) $\frac{t_1, \cdots, t_n}{ft_1, \cdots, t_n}$ if n-ary $f \in S$

Remark. if $\mathfrak{C}$ defines Z, we can prove assertions about all elements of Z by means of induction over $\mathfrak{C}$
(this principle of proof corresponds to induction over $\mathbb{N}$)

Claim. *To show that all elements of Z (defined by $\mathfrak{C}$) have a certain property P*
it is sufficient to show
(I) for every rule $\frac{\zeta_1, \cdots, \zeta_n}{\zeta}$ of $\mathfrak{C}$, the following holds:
(induction hypothesis) whenever $\zeta_1, \cdots, \zeta_n$ are derivable in $\mathfrak{C}$ and have some property P
then then ζ also has property P
eg case $n = 0$, must show that ζ has property P

Proof. This method is justified using principle of complete induction for $\mathbb{N}$
Define length of a derivation in $\mathfrak{C}$ to be like those in section 2.3.
If condition I is satisfied for P, show by induction on m (=the length of derivation in $\mathfrak{C}$) that every string which has a derivation of length m has the property P. Since every element of Z has a derivation of some finite length, P must hold for all elements of Z

Example.
- $Z = T^S$
  to show all S-terms have a certain property P, it is sufficient to show ("proof by induction on terms"):
  (T1)' every variable has property P
  (T2)' every constant in S has property P
  (T3)' if S-terms $t_1, \cdots, t_n$ have the property P, and if $f \in S$ is n-ary, then $ft_1, \cdots, t_n$ also has property P
- $Z = L^S$
  to show all S-formulas have a certain property P, it is sufficient to show ("proof by induction on formuals"):
  (F1)' every S-formuala of the form $t_1 \equiv t_1$ has property P
  (F2)' every S-formuala of the form $Rt_1 ... t_n$ has property P
  (F3)' if the S-formula ϕ has property P, then $\neg\phi$ also has property P
  (F4)' if the S-formulas ϕ and ψ have property P, then $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \to \psi)$, $(\phi \leftrightarrow \psi)$ also have property P
  (F5)' if the S-formulas ϕ has property P and x is a variable, then $\forall x\phi$ and $\exists x\phi$ also have property P

Remark. next some applications of this method of proof

Claim. *4.1*
(a) for all symbol sets S, the empty string $\square$ is neither a S-term nor a S-formula
(b1) $\circ$ is not a S_{gr}-term
(b2) $\circ \circ v_1$ is not a S_{gr}-term
(c) for all symbol sets S, every S-formula contains the same number of right parenteses) as of left parentheses (

Proof.
(a) Let P be the property on A_S^* to hold for string ζ iff ζ non-empty
Will show by induction on terms that every S-term has property P
(T1)',(T2)': terms of form x or c (where $c \in S$) are nonempty
(T3)': every term begins with function symbol thus nonempty (note: didnt need induction hypothesis)
formulas are analogous
(b) 1) left to reader
2) Let P be the property on $A_{S_{gr}}^*$ which holds for string ζ iff ζ is distinct from $\circ \circ v_1$
$t = x, t = c$: t is distinct from $\circ \circ v_0$
$t = \circ t_1 t_2$: if $\circ t_1 t_2 = \circ \circ v_1$, then by (a), $t_1 = \circ$ and $t_2 = v_1$
but $t_1 = \circ$ contradicts (1)
(c) First show by induction on terms that no S-term contains a left or right parenthesis.
Then consider the property P over A_S^* which holds for string $\zeta \in A_S^*$ iff ζ has same number of left,right parentheses
Then show by induction on formulas that every S-formula has the property P
case $\phi = t_1 \equiv t_2$: showed above that terms have no parentheses. thus P holds for ϕ
case $\phi = \neg\psi$ where (by induction hypothesis) ψ has P. ϕ only contains those parentheses in ψ, so P holds for ϕ
case $\phi = (\psi \wedge \chi)$ where (by induction hypothesis) P holds for ψ, χ: ϕ has those parentheses in ψ, χ and two more, so P holds for ϕ
rest of cases are just like ones above

Remark. Next will show that terms and formulas have a unique decomposition. But first two lemmas. All consider some fixed symbol set S.

Lemma. *4.2*
(a) for all terms t and t', t is not a proper initial segment of t' (ie there is no ζ distinct from $\square$ st $t\zeta = t'$)
(b) for all formulas ϕ and ϕ', ϕ is not a proper initial segment of ϕ'

Proof. (a) consider property P that holds for string η iff
(*) $\forall$ terms t', t' is not a proper initial segment of η and η is not a proper initial segment of t'
Will use induction on terms to show all terms have property P
Case $t = x$: 4.1a $\Rightarrow t'$ cant be a proper initial segment of x for then t would be $\square$
on the other hand, can show by induction on terms that x is the only term that begins with x
therefore, t cant be a proper initial segment of x
Case $t = c$: similar argument
Case $t = ft_1 ... t_n$ and (*) holds for $t_1, ..., t_n$:
Fix arbitrary term t'.
Will show t' cant be a proper initial segment of t
otherwise there would be ζ st
$\zeta \neq \square, t = t'\zeta$
since t' begins with f (since t begins with f), t' cant be a variable or a constant
thus t' must have been generated using (T3)
Thus it has the form
$ft_1 ... t_n = ft_1' ... t_n'\zeta$
and by cancelling symbol f, $t_1 ... t_n = t_1' ... t_n'\zeta$
Therefore t_1 is an initial segment of t_1' or vice versa but neither can be proper initial segments of the other since t_1 satisfies (*) by induction hypothesis
thus $t_1 = t_1'$
cancelling, we get $t_2 ... t_n = t_2' ... t_n'\zeta$
repeating this argument, we finally obtain $\square = \zeta$
this contradicts $\zeta \neq \square$
thus t' cant be proper initial segment of t
proof that t cant be proper initial segment of t' is analgous
(b) analogous

Lemma. *4.3*
(a) if $t_1, \cdots, t_n$ and $t_1', \cdots, t_m'$ are terms and if $t_1 \cdots t_n = t_1' \cdots t_m'$
then $m = n$ and $t_i = t_i'$ for $1 \leq i \leq n$
(b) if $\phi_1, \cdots, \phi_n$ and $\phi_1', \cdots, \phi_m'$ are formulas and if $\phi_1 \cdots \phi_n = \phi_1' \cdots \phi_m'$
then $m = n$ and $\phi_i = \phi_i'$ for $1 \leq i \leq n$

Proof. similar to pf of lem 4.2

Theorem. *4.4 ["unique readability"]*
(a) every term is either a variable or a constant or a term of the form $ft_1 \cdots t_n$. In the last case, the function symbol f and the terms $t_1, \cdots, t_n$ are uniquely determined
(b) every formula has the form either (1) $t_1 \equiv t_2$, (2) $Rt_1 \cdots t_n$, (3) $\neg\phi$, (4) $(\phi \wedge \psi)$, (5) $(\phi \vee \psi)$, (6) $(\phi \to \psi)$, (7) $(\phi \leftrightarrow \psi)$, (8) $\forall x\phi$, or (9) $\exists x\phi$ where cases (1)-(9) are mutually exclusive and where the following are uniquely determined: the terms t_1, t_2 in case (1), the relation symbol R and terms $t_1, \cdots, t_n$ in case (2), the formulas ϕ, ψ in cases (3)-(7), and the variable x and formula ϕ in (8),(9)

Proof. use lem 4.2,4.3

Definition.
- inductive definition on terms to define a function for all terms, it is sufficient to:
  (T1)" assign a value to each variable
  (T2)" assign a value to each constant
  (T3)" for every n-ary f and for all terms $t_1, \cdots, t_n$ to assign a value to the term $ft_1, \cdots, t_n$ assuming that values have already been assigned to the terms $t_1, \cdots, t_n$
- inductive definition on formulas is analogous

Claim. *each term is assigned exactly one value by (T1)"-(T3)"*

Proof. using induction on terms to show each term is assigned exactly one value by (T1)"-(T3)"
case $t = x$: by thm4.4a t is not const and does not begin with a function symbol. Thus it is assigned a value by an application of (T1)". Thus t is assigned exactly one value.
case $t = c$: analogous to above case
case $t = ft_1, \cdots, t_n$ where each $t_1, \cdots, t_n$ has been assigned exactly one value:
to assign a value to t, can only use (T3)", by thm4.4a. Since, again by thm4.4a, the t_i are uniquely determined, t is assigned a unique value

Remark. will now give some inductive definitions

Definition.
- the function var (more precisely, var_S) associates with each S-term the set of variables occuring in it, can be defined as follows:
  $\text{var}(x) := \{x\}$
  $\text{var}(c) := \emptyset$
  $\text{var}(ft_1 \cdots t_n) := \text{var}(t_1) \cup \cdots \cup \text{var}(t_n)$
- the function SF assigns to each formula the set of its subformaulas, can be defined by induction on formulas as follows:
  $SF(t_1 \equiv t_2) := \{t_1 \equiv t_2\}$
  $SF(Rt_1 \cdots t_n) := \{Rt_1 \cdots t_n\}$
  $SF(\neg\phi) := \{\neg\phi\} \cup SF(\phi)$
  $SF((\phi * \psi)) := \{(\phi * \psi)\} \cup SF(\phi) \cup SF(\psi)$ for $* = \wedge, \vee, \to, \leftrightarrow$
  $SF(\forall x\phi) := \{\forall x\phi\} \cup SF(\phi)$
  $SF(\exists x\phi) := \{\exists x\phi\} \cup SF(\phi)$

Remark. can define preceding notions by calculi, see exersize 4.6

2.5. FREE VARIABLES AND SENTENCES.

Definition.
- free variables ("parameters") are not quantified ie not in the scope of a corresponding quantifier
- bound variables are quantified
- sentence is a formula without free variables (parameter-free)
  eg $\exists v_0 \neg v_0 \equiv v_0$ is a sentence
- L_n^S is the set of S-formulas in which the variables occuring free are among $v_0, \cdots, v_{n-1}$
  ie $L_n^S := \{\phi | \phi \text{ is an } S\text{-formula and free}(\phi) \subset \{v_0, \cdots, v_{n-1}\}\}$
  eg L_0^S is the set of S-sentences

Remark. variables can have both free and bound occurances in same formula, eg $S = \{R\}$, $\phi := \exists x(Ryz \wedge \forall y(\neg y \equiv x \vee Ryz))$, x is bound, z is free, and y has both free and bound occurances

Definition. let set free(ϕ) be the set of free variables in formula ϕ. A definition by induction on formulas is, for fixed S,
free$(t_1 \equiv t_2) :=$ var$(t_1) \cup$ var(t_2)
free$(Pt_1 \cdots t_n) :=$ var$(t_1) \cup \cdots \cup$ var(t_n)
free$(\neg\phi) :=$ free(ϕ)
free$(\phi_1 * \phi_2) :=$ free$(\phi_1) \cup$ free(ϕ_2) where $* = \wedge, \vee, \rightarrow, \leftrightarrow$
free$(\forall x\phi) :=$ free$(\phi) \setminus \{x\}$
free$(\exists x\phi) :=$ free$(\phi) \setminus \{x\}$

Example.
- use this definition to determine set of free variables in ψ from recent remark
- simpler example: let x, y, z be distinct, then free$((Ryx \rightarrow \forall y \neg y \equiv z)) =$ free$(Ryx) \cup$ free$(\forall y \neg y \equiv z) = \{x, y\} \cup (\{y, z\} \setminus \{y\}) = \{x, y, z\}$

3. SEMANTICS OF FIRST ORDER LANGUAGES

Remark.
- a formula has no meaning attached
- this chapter:
  -formulation of the notion of interpretation of symbols in formula
  -define when an interpretation yields a true and false statement
  -define the consequence relation
- ch2: syntactic concepts - involve only grammatical properties of symbol strings
  ch3: semantic concepts - depend on the meanings of symbol strings

Example.
- $\{R\}$-formula $\forall v_0 Rv_0 v_0$ has no meaning attached
  -let domain $\mathbb{N}$, then $\forall v_0$ means "for all $v_0 \in \mathbb{N}$", and let R be the divisibility relation $R^{\mathbb{N}}$ on $\mathbb{N}$. Then the formula holds (is true) in $(\mathbb{N}, R^{\mathbb{N}})$
  -let domain $\mathbb{Z}$, then $\forall v_0$ means "for all $v_0 \in \mathbb{Z}$", and let R be less relation $R^{\mathbb{Z}}$ (ie $<$) on $\mathbb{Z}$. then the formula does not hold in $(\mathbb{Z}, R^{\mathbb{Z}})$
- $\{R\}$-formula $\exists v_0 (Rv_1 v_0 \wedge Rv_0 v_2)$ in $(\mathbb{Z}, R^{\mathbb{Z}})$
  holds when $v_1 = 5, v_2 = 8$
  does not hold when $v_1 = 5, v_2 = 6$

3.1. STRUCTURES AND INTERPRETATIONS.

Definition.
- n-ary function on set A is a map with domain A^n, $n \geq 1$, of n-tuples and whose value lies in A
- n-ary relation R is a subset of A^n
  ie $Ra_1 \cdots a_n$ means $(a_1, \cdots, a_n) \in R$
  say "relation R holds for $a_1, \cdots, a_n$"
- S-structure is a pair $\mathfrak{A} = (A, \mathfrak{a})$ with properties
  a) A is nonempty set, the domain or universe of $\mathfrak{A}$
  b) $\mathfrak{a}$ is a map defined on S satisfying
  b1) $\forall n$-ary relation symbols R in S, $\mathfrak{a}(R)$ is an n-ary relation symbol on A
  b2) $\forall n$-ary function symbols f in S, $\mathfrak{a}(f)$ is an n-ary function symbol on A
  b3) $\forall$ const $c \in S$, $\mathfrak{a}(c)$ is an element of A

Remark. notation:
- $\mathfrak{a}(R)$, $\mathfrak{a}(f)$, $\mathfrak{a}(c)$ will be written $R^{\mathfrak{A}}$, $f^{\mathfrak{A}}$, $c^{\mathfrak{A}}$, or simply R^A, f^A, c^A
- structures $\mathfrak{A}, \mathfrak{B}, \cdots$ will use $A, B, \cdots$ to denote their domains
- will replace $\mathfrak{a}$ with a list of values
  eg $\{R, f, g\}$-structure $\mathfrak{A} = (A, R^{\mathfrak{A}}, f^{\mathfrak{A}}, g^{\mathfrak{A}})$

Example. structures
- $\{R\}$-structure $(\mathbb{N}, R^{\mathbb{N}})$ where R^N is divisibility relation $\{(n, m) | \exists k \in \mathbb{N} \; st \; n \cdot k = m\}$
- $\{R\}$-structure $(\mathbb{Z}, R^{\mathbb{Z}})$ where R^Z is less than relation
- S_{gr}-structure $(\mathbb{R}, +, 0)$ where $\circ$ is $+$ over $\mathbb{R}$ and e is 0
- Let arithmetic symbol sets $S_{ar} := \{+, \cdot, 0, 1\}$ and $S_{ar}^{<} := \{+, \cdot, 0, 1, <\}$ where $+, \cdot$ are binary function symbols, 0,1 are consts, and $<$ is binary relation
  - S_{ar}-structure $\mathfrak{N} := (\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}})$ where $+^{\mathbb{N}}, \cdot^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}}$ are the usual plus and times over $\mathbb{N}$ and numbers 0 and 1
  - S_{ar}-structure $\mathfrak{N}^{<} := (\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}}, <^{\mathbb{N}})$ where $<^{\mathbb{N}}$ denotes the usual ordering on $\mathbb{N}$
  - S_{ar}-structures $\mathfrak{R}$ and $\mathfrak{R}^{<}$ analogous for domain $\mathbb{R}$

  notation: can drop superscripts $\mathbb{N}, \mathbb{R}$ when unambiguous

Definition.
- assignment in S-structure $\mathfrak{A}$ is map $\beta : \{v_n | n \in \mathbb{N}\} \rightarrow A$ of a set of variables into the domain A
- S-interpretation $\mathfrak{I}$ is pair $(\mathfrak{A}, \beta)$ where $\mathfrak{A}$ is structure and β is assignment in $\mathfrak{A}$
- for given β, assignment $\beta\frac{a}{x}$ agrees with β except x is assigned a
  ie $\beta\frac{a}{x}(y) := \beta(y)$ if $y \neq x$ and a if $y = x$
- for given $\mathfrak{I} = (\mathfrak{A}, \beta)$, define $\mathfrak{I}\frac{a}{x} := (\mathfrak{A}, \beta\frac{a}{x})$

Example. given S-interpretation, can read S-formula in everyday language:
eg $S_{ar}^{<}$-interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ given by
$\mathfrak{A} = (\mathbb{N}, +, \cdot, 0, 1, <)$ and $\beta(v_n) = 2n$ for $n \geq 0$
then
- formula $\cdot v_2 + v_1 v_2 \equiv v_4$ (shorthand $v_2 \cdot (v_1 + v_2) \equiv v_4$) is read $4 \cdot (2 + 4) = 8$
- formula $\forall v_0 \exists v_1 < v_0 v_1$ (shorthand $\forall v_0 \exists v_1 v_0 < v_1$) is read "for every natural number there is a larger natural number"

3.2. STANDARDIZATION OF CONNECTIVES.

Definition. $\dot{\vee}, \dot{\wedge}, \dot{\rightarrow}, \dot{\leftrightarrow}$ are functions : $\{T, F\} \times \{T, F\} \rightarrow \{T, F\}$ st truth table

		$\dot{\vee}$	$\dot{\wedge}$	$\dot{\rightarrow}$	$\dot{\leftrightarrow}$
T	T	T	T	T	T
T	F	T	F	F	F
F	T	T	F	T	F
F	F	F	F	T	T

$\dot{\neg}$ is function : $\{T, F\} \rightarrow \{T, F\}$ st

	$\dot{\neg}$
T	F
F	T

Remark. extensional use of connectives - truth values of compound propositions only depend on truth values of constituents
intensional use of connectives - truth values of compound statements also depend on the order of the two components
we restruct ourselves to extensional
will see (§11.4) that all other extensional connectives can be defined from the connectives we have chosen

3.3. THE SATISFACTION RELATION.

Remark.
- want to make precise the notion of a formula being true under an interpretation
- henceforth, fix S and drop prefix $S-$

Definition. given $\mathfrak{I}(\mathfrak{A}, \beta)$, define, by induction on terms, $\mathfrak{I}(t) \in A$ for each term t,
a) for variable x, $\mathfrak{I}(x) := \beta(x)$
b) for const $c \in S$, $\mathfrak{I}(c) := c^{\mathfrak{A}}$
c) for any n-ary function symbol $f \in S$ and terms $t_1, \cdots, t_n$, let $\mathfrak{I}(ft_1 \cdots t_n) := f^{\mathfrak{A}}(\mathfrak{I}(t_1), \cdots, \mathfrak{I}(t_n))$

Example. S_{gr}, $\mathfrak{I}(\mathfrak{A}, \beta)$, $\mathfrak{A} = (\mathbb{R}, +, 0)$, $\beta(v_0) = 2$, $\beta(v_2) = 6$
then $\mathfrak{I}(v_0 \circ (e \circ v_2)) = \mathfrak{I}(v_0) + \mathfrak{I}(e \circ v_2) = 2 + (0 + 6) = 8$

Definition.
- given interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$, define, by induction on formulas ϕ, relation $\mathfrak{I} \models \phi$, $\mathfrak{I}$ satisfies ϕ ("$\mathfrak{I}$ is a model of ϕ", "ϕ holds in $\mathfrak{I}$")

$\mathfrak{I} \models t_1 \equiv t_2 \quad : iff \quad \mathfrak{I}(t_1) = \mathfrak{I}(t_2)$

$\mathfrak{I} \models Rt_1 \cdots t_2 \quad : iff \quad R^{\mathfrak{A}}\mathfrak{I}(t_1) \cdots \mathfrak{I}(t_2)$

$\mathfrak{I} \models \neg\phi \quad : iff \quad$ not $\mathfrak{I} \models \phi$

$\mathfrak{I} \models (\phi \wedge \psi) \quad : iff \quad \mathfrak{I} \models \phi$ and $\mathfrak{I} \models \psi$

$\mathfrak{I} \models (\phi \vee \psi) \quad : iff \quad \mathfrak{I} \models \phi$ or $\mathfrak{I} \models \psi$

$\mathfrak{I} \models (\phi \rightarrow \psi) \quad : iff \quad \mathfrak{I} \models \phi$ then $\mathfrak{I} \models \psi$

$\mathfrak{I} \models (\phi \leftrightarrow \psi) \quad : iff \quad \mathfrak{I} \models \phi$ iff $\mathfrak{I} \models \psi$

$\mathfrak{I} \models \forall x\phi \quad : iff \quad$ for all $a \in A, \mathfrak{I}\frac{a}{x} \models \phi$

$\mathfrak{I} \models \exists x\phi \quad : iff \quad$ there is an $a \in A, \mathfrak{I}\frac{a}{x} \models \phi$

- $\mathfrak{I}$ is a model of a set of S-formulas Φ, $\mathfrak{I} \models \Phi$, means $\mathfrak{I} \models \phi$ for all $\phi \in \Phi$

Remark.
- $: iff$ means left side is defined by right side
- intuition: $\mathfrak{I} \models \phi$ iff ϕ is true statement under interpretation $\mathfrak{I}$

Example. S_{gr}, $\mathfrak{I} = (\mathfrak{A}, \beta)$, $\mathfrak{A} = (\mathbb{R}, +, 0)$, $\beta(x) = 9$
$\forall x$
thus $\mathfrak{I} \models \forall v_0 v_0 \circ e \equiv v_0$
iff for all $r \in \mathbb{R}$, $\mathfrak{I}\frac{r}{v_0} \models v_0 \circ e \equiv v_0$
iff for all $r \in \mathbb{R}$, $r + 0 = r$

3.4. THE CONSEQUENCE RELATION.

Remark.
- will state exactly when a formula is a consequence of a set of formulas
- continue letting S fixed symbol set

Definition. formula ϕ is a consequence of set of formulas Φ, $\Phi \models \phi$, :iff every interpretation which is a model of Φ is also a model of ϕ

Remark. notation:
- $\models$ is used for satisfaction relation and consequence relation, known from context
- for singleton $\Phi = \{\psi\}$, write $\psi \models \phi$

Example. clm 1.1.1 ($\exists$ of left inverse in groups)
$\Phi_{gr} \models \forall v_0 \exists v_1 v_1 \circ v_0 \equiv e$
(where $\Phi_{gr} = \{\forall v_0 \forall v_1 \forall v_2 (v_0 \circ v_1) \circ v_2 \equiv v_0 \circ (v_1 \circ v_1), \forall v_0 v_0 \circ e \equiv v_0, \forall v_0 \exists v_1 v_0 \circ v_1 \equiv e\}$

Remark. to show ϕ is not a consequence of Φ, it is sufficient to give an interpretation which satisfies every formula in Φ but fails to satisfy ϕ

Example.
- show: not $\Phi_{gr} \models \forall v_0 \forall v_1 v_0 \circ v_1 \equiv v_1 \circ v_0$ ie commutative
  give interpretation of nonabelian group $\mathfrak{G}$ with arbitrary assignment of variables
- show: not $\Phi_{gr} \models \neg\forall v_0 \forall v_1 v_0 \circ v_1 \equiv v_1 \circ v_0$
  give interpretation of an abelian group
- from these two examples, see that not $\Phi \models \phi$ does not necessarily imply $\Phi \models \neg\phi$

Remark. To what extent can the consequence of a system of axioms be obtained by means of a mathematical proof? see ch 5 (preview: yes, consequence relation $\Phi \models \phi$ can always be established by means of a mathematical proof. This proof consists of steps which can be described formally (syntactically))

Definition.
- valid formula ϕ, "$\models \phi$", :iff $\emptyset \models \phi$
  ie holds under all interpretations
  eg $(\phi \vee \neg\phi)$ and $\exists x x \equiv x$ are both valid
- satisfiable formula ϕ, Sat ϕ, iff $\exists$ interpretation which is a model of ϕ
- satisfiable set of formulas Φ, Sat Φ, iff $\exists$ interpretation which is a model for all formulas in Φ

Lemma. *4.4*
for all Φ and all ϕ,
$\Phi \models \phi$ iff not Sat $\Phi \cup \{\neg\phi\}$
in particular, ϕ is valid iff $\neg\phi$ is not satisfiable

Proof. book

Definition. two logically equivalent formulas ϕ and ψ, $\phi \dashv\models \psi$, iff $\phi \models \psi$ and $\psi \models \phi$

Remark. thus, logically equivalent iff valid under the same interpretations ie iff $\models \phi \leftrightarrow \psi$

Example. logically equivalent formulas:
$\phi \wedge \psi$ and $\neg(\neg\phi \vee \neg\psi)$
$\phi \to \psi$ and $\neg\phi \wedge \psi$
$\phi \leftrightarrow \psi$ and $\neg(\phi \vee \psi) \vee \neg(\neg\phi \vee \neg\psi)$
$\forall x\phi$ and $\neg\exists x\neg\phi$
Pf: truth tables

Remark.
- using above example, can dispense with $\wedge, \to, \leftrightarrow, \forall$ without losing expressive power
- can define map $*$ by induction on formulas which take formula ϕ to logically equivalent formula ϕ^* which has no $\wedge, \to, \leftrightarrow, \forall$ using example above (see book for definition of ϕ^* by induction on formulas)
- this simplifies eg proof by induction on formulas, def of formula, def of satisfaction
- will still use $\wedge, \to, \leftrightarrow, \forall$ as short hand notation

Definition. $\mathfrak{I}_1, \mathfrak{I}_2$ agree on variable x means $\beta_1(x) = \beta_2(x)$
and on symbol k means $k^{\mathfrak{A}_1} = k^{\mathfrak{A}_2}$.

Lemma. *(4.6) (coincidence lemma)*
Let S_1-interpretation $\mathfrak{I}_1 = (\mathfrak{A}_1, \beta_1)$ and S_2-interpretation $\mathfrak{I}_2 = (\mathfrak{A}_2, \beta_2)$ and $A_1 = A_2$ ie same domain.
Put $S = S_1 \cap S_2$
a) Let S-term t. If $\mathfrak{I}_1$ and $\mathfrak{I}_2$ agree on the S-symbols occuring in t and variables occuring in t, then $\mathfrak{I}_1(t) = \mathfrak{I}_2(t)$
b) Let S-formula ϕ. If $\mathfrak{I}_1$ and $\mathfrak{I}_2$ agree on the S-symbols occuring in ϕ and on the variables occuring free in ϕ, then $\mathfrak{I}_1 \models \phi$ iff $\mathfrak{I}_2 \models \phi$

Proof. see book

Remark.
- in particular, coincidence lemma says: the validity of S-formula ϕ under S-interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ depends only on the assignments of the finitely many variables occuring free in ϕ (and of course on the interpretation of the symbols of S in $\mathfrak{I}$)
- notation:
  - if free variables of ϕ are among $v_0, \cdots, v_n$, ie $\phi \in L_n^S$, then at most the β-values $\beta(v_i) = a_i$, $i = 0, \cdots, n-1$, are significant
    denote $(\mathfrak{A}, \beta) \models \phi$ with $\mathfrak{A} \models \phi[a_0, \cdots, a_{n-1}]$
  - for S-term t st $\mathrm{var}(t) = \{v_0, \cdots, v_{n-1}\}$, write $t^{\mathfrak{A}}[a_1, \cdots, a_{n-1}]$ instead of $\mathfrak{I}(t)$
  - if ϕ is a sentence, write $\mathfrak{A} \models \phi$ and say "$\mathfrak{A}$ is a model for ϕ"
  - if Φ is set of sentences, write $\mathfrak{A} \models \Phi$ which means $\mathfrak{A} \models \phi$ for all $\phi \in \Phi$

Definition.
- Let S-structure $\mathfrak{A}$, S'-structure $\mathfrak{A}'$
  $\mathfrak{A}$ is a reduct of $\mathfrak{A}'$ ("$\mathfrak{A} = \mathfrak{A}'|_S$") means
  $S \subset S'$, $A = A'$, and $\mathfrak{a}, \mathfrak{a}'$ agree on S
- $\mathfrak{A}'$ is a expansion of $\mathfrak{A}$ has same def

Example. $S_{ar}^{<}$-structure $\mathfrak{R}^<$ (ordered field of real numbers) is an expansion of S_{ar}-structure $\mathfrak{R}$ (field of real numbers)
ie $\mathfrak{R} = \mathfrak{R}^<|_S$

Claim. *let $\mathfrak{A} = \mathfrak{A}'|_S$, $\phi \in L_n^S$, and $a_0, \cdots, a_{n-1} \in A$*
$\mathfrak{A} \models \phi[a_0, \cdots, a_{n-1}]$ iff $\mathfrak{A}' \models \phi[a_0, \cdots, a_{n-1}]$

Proof. coincidence lemma, see book

Remark. interpretation, consequence, and satisfiability refer to a fixed symbol set S
can remove this reference to S using concidence lemma.
next clm does this for satisfiability

Claim. *Let set of S-formulas Φ, $S \subset S'$, note that Φ is also set of S'-formulas*
Φ is satisfiable wrt S iff Φ is satisfiable wrt S'

Proof. see book

Remark. history: semantics is due to Tarski; and logical consequence was already present in work of Bolzano

3.5. TWO LEMMAS ON THE SATISFACTION RELATION.

Remark. now, results about isomorphic structures and substructures

Definition. Let S-structures $\mathfrak{A}$ and $\mathfrak{B}$
- isomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$ is a map $\pi : A \to B$ ("$\pi : \mathfrak{A} \cong \mathfrak{B}$") :iff
  1) π is a bijection of A and B
  2) For n-ary $R \in S$ and $a_1, \cdots, a_n \in A$,
  $R^{\mathfrak{A}} a_1 \cdots a_n$ iff $R^{\mathfrak{B}} \pi(a_1) \cdots \pi(a_n)$
  3) For n-ary $f \in S$ and $a_1, \cdots, a_n \in A$,
  $\pi(f^{\mathfrak{A}}(a_1, \cdots, a_n)) = f^{\mathfrak{B}}(\pi(a_1), \cdots, \pi(a_n))$
  4) for $c \in S$, $\pi(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$
- isomorphic structures A and B, $A \cong B$
  iff there is an isomorphism $\pi : \mathfrak{A} \cong \mathfrak{B}$

Example. are S_{gr}-structures $(\mathbb{N}, +, 0)$ and $(G, +^G, 0)$ (where G = {even natural numbers} and $+^G$ is ordinary addition) isomorphic?
Yes, with isomorphism $\pi : \mathbb{N} \to G$, $\pi(n) = 2n$

Lemma. *(isomorphism lemma)*
Let S-structures $\mathfrak{A} \cong \mathfrak{B}$, S-sentence ϕ
then $\mathfrak{A} \models \phi$ iff $\mathfrak{B} \models \phi$

Proof. induction on terms, induction on formulas, see book

Corollary. *Let $\pi : \mathfrak{A} \cong \mathfrak{B}$, $\phi \in L_n^S$ and $a_0, \cdots, a_{n-1} \in A$*
$\mathfrak{A} \models \phi[a_0, \cdots, a_{n-1}]$ iff $\mathfrak{B} \models \phi[\pi(a_0), \cdots, \pi(a_{n-1})]$

Remark.
- isomorphic structures cannot be distinguished in L_0^S
- conversely, can S-structures in which the same S-sentences are satisfied be isomorphic? (not always, see ch4. eg there are structures not isomorphic to the S_{ar}-structure $\mathfrak{N}$ of natural numbers in which the same first order sentences hold)

Example.
- in the rational numbers, every number n is divisible by 2:
  $(\mathbb{Q}, +, 0) \models \forall v_0 \exists v_1 v_1 + v_1 \equiv v_0$
- in the integers, this is not true:
  not $(\mathbb{Z}, +, 0) \models \forall v_0 \exists v_1 v_1 + v_1 \equiv v_0$

Remark.
- so sentences might no longer hold when passing to substructures
- rest of section: introduce substructures; give a class of sentences preserved by substructures

Definition. Let S-structures $\mathfrak{A}$ and $\mathfrak{B}$
$\mathfrak{A}$ is a substructure of $\mathfrak{B}$ ("$\mathfrak{A} \subset \mathfrak{B}$") means
a) $A \subset B$
b1) for n-ary $R \in A$, $R^{\mathfrak{A}} = R^{\mathfrak{B}} \cap A^n$
ie for all $a_1, \cdots, a_n \in A$, $R^{\mathfrak{A}} a_1 \cdots a_n$ iff $R^{\mathfrak{B}} a_1 \cdots a_n$
b2) for n-ary $f \in S$, $f^{\mathfrak{A}}$ is the restriction of $f^{\mathfrak{B}}$ to A^n
b3) for $c \in S$ $c^{\mathfrak{A}} = c^{\mathfrak{B}}$

Example.
- $(\mathbb{Z}, +, 0)$ is a substructure of $(\mathbb{Q}, +, 0)$ (and a subgroup)
- $(\mathbb{N}, +, 0)$ is a substructure of $(\mathbb{Z}, +, 0)$ (but not a subgroup, nor a group)

Definition. A is S-closed in $\mathfrak{B}$ means
- $A \subseteq B$ is nonempty
- for n-ary $f \in S$, $a_1, \cdots, a_n \in A$: $f^{\mathfrak{B}}(a_1, \cdots, a_n) \in A$
- for $c \in S$: $c^{\mathfrak{B}} \in A$

Claim.
- *if $\mathfrak{A} \subset \mathfrak{B}$ then $\mathfrak{A}$ is S-closed in $\mathfrak{B}$*
- *conversely, every subset X of B which is S-closed in $\mathfrak{B}$ is the domain of exactly one substructure of $\mathfrak{B}$*
  (condition b in def of substructure determines exactly one structure with domain X
  call it the substructure generated by X in $\mathfrak{B}$, denote it $[X]^{\mathfrak{B}}$)

Example.
- set $\{2n | n \in \mathbb{N}\}$ (ie even naturals) is S_{gr}-closed in $(\mathbb{Z}, +, 0)$
- set $\{2n+1 | n \in \mathbb{N}\}$ is not S_{gr}-closed, since 3+3 is even

Definition. quantifier-free formula does not contain any quantifiers

Lemma. *let S-structures $\mathfrak{A} \subset \mathfrak{B}$ and let $\beta : \{v_n | n \in \mathbb{N}\} \to A$ be an assignment in $\mathfrak{A}$*
a) for every S-term t, $(\mathfrak{A}, \beta)(t) = (\mathfrak{B}, \beta)(t)$
b) for every quantifier-free S-formula ϕ
$(\mathfrak{A}, \beta) \models \phi$ iff $(\mathfrak{B}, \beta) \models \phi$

Proof. easy, left to reader, follows from proof of isomorphism lemma by leaving out existential quantifier and choosing map $\pi : A \to B$ to be identity $\pi(a) = a$ for all $a \in A$

Example. (this ex motivates next def and lem)
Let group $\mathfrak{B}$ and substructure $\mathfrak{A}$
associative law $\forall v_0 \forall v_1 \forall v_2 (v_0 \circ v_1) \circ v_2 \equiv v_0 \circ (v_1 \circ v_2)$ holds also in $\mathfrak{A}$
pf: $(a \circ^{\mathfrak{B}} b) \circ^{\mathfrak{B}} c = a \circ^{\mathfrak{B}} (b \circ^{\mathfrak{B}} c)$ holds even for all $a, b, c \in B$ and $\circ^{\mathfrak{B}}$ on A agrees with $\circ^{\mathfrak{A}}$

Remark. this formula for associative law is "universal" (following def)

Definition. universal formulas are derivable by means of the calculus
i) $\frac{}{\phi}$ if ϕ is quantifier-free
ii) $\frac{\phi, \psi}{(\phi * \psi)}$ for $* = \wedge, \vee$
iii) $\frac{\phi}{\forall x \phi}$

Remark. every universal formula is logically equivalent to a formula of the form $\forall x_1 \cdots \forall x_n \psi$ with quantifier-free ψ (see pf of 8.4.4)

Lemma. *(substructure lem)*
Let S-structures $\mathfrak{A} \subset \mathfrak{B}$, let $\phi \in L_n^S$ be universal, and let $a_0, \cdots, a_{n-1} \in A$
if $\mathfrak{B} \models \phi[a_0, \cdots, a_{n-1}]$ then $\mathfrak{A} \models \phi[a_0, \cdots, a_{n-1}]$

Proof. see book

Corollary. *Let structures $\mathfrak{A} \subset \mathfrak{B}$*
for every universal sentence ϕ
if $\mathfrak{B} \models \phi$ then $\mathfrak{A} \models \phi$

Example.
- substructure $(\mathbb{N}, +, 0)$ of group $(\mathbb{Z}, +, 0)$ is itself not a group
  Cor shows that cannot be a system of axioms for group theory in $L^{S_{gr}}$ consisting only of universal sentences
- however, for $S_{grp} := \{\circ, ^{-1}, e\}$ where unary func $^{-1}$ is inverse map
  the axioms $\Phi_{grp} := \{\forall v_0 \forall v_1 \forall v_2 (v_0 \circ v_1) \circ v_2 \equiv v_0 \circ (v_1 \circ v_2), \forall v_0 v_0 \circ e \equiv v_0, \forall v_0 v_0 \circ v_0^{-1} = e\}$
  consists only of unversal sentences.
  For groups as S_{grp}-structures, substructures and subgroups coincide

3.6. SOME SIMPLE FORMULATIONS.

Definition. formalize a theory means its axioms can be formulated in first-order language

Remark.
- this section: will formalize some theories
- since variable symbols dont matter (eg can replace v_0 with v_{100} everywhere), will use (distinct) variables x, y, z

Example. group theory
- recall axioms Φ_{gr} from §3.4
- can also formalize cancellation law for group theory
  $\phi := \forall x \forall y \forall z (x \circ z \equiv y \circ z \to x \equiv y)$
  cancellation law holds in particular interpretation $\mathfrak{G}$ means $\mathfrak{G} \models \phi$
  cancellation law holds in all groups means $\Phi_{gr} \models \phi$
- can formalize statement "there is no formula of order 2"
  $\psi := \neg \exists x (\neg x \equiv e \wedge x \circ x \equiv e)$
  group $(\mathbb{Z}, +, 0)$ is a model of ψ since it has no elements of order 2

Example. equivalence relation theory
- $\forall x R x x$
  $\forall x \forall y (Rxy \to Ryx)$
  $\forall x \forall y \forall z ((Rxy \wedge Ryz) \to Rxz)$
- thm in §1.2 (if x and y are equivalent to a third element, then they are equivalent to the same elements) is formalized:
  $\forall x \forall y (\exists u (Rxu \wedge Ryu) \to \forall z (Rxz \leftrightarrow Ryz))$

Example. continuity
- Let unary func ρ on $\mathbb{R}$ and binary distance func Δ on $\mathbb{R}$ $\Delta(r_0, r_1) = |r_0 - r_1|$ for all $r_0, r_1 \in \mathbb{R}$
- can treat $(\mathbb{R}, +, \cdot, 0, 1, <, \rho, d)$ as an $S_{ar}^{<} \cup \{f, d\}$-structure where function symbols f, d for ρ, Δ
- the contunuity of ρ on $\mathbb{R}$ is stated: for all x and for all $\epsilon > 0$, there is a $\delta > 0$ st for all y, if $\Delta(x, y) < \delta$ then $\Delta(\rho(x), \rho(y)) < \epsilon$
- formalize using variables u and v for ϵ and δ:
  $\forall x \forall u (0 < u \to \exists v (0 < v \wedge \forall y (dxy < v \to dfxfy < u))$

Remark.
- statements of form "for all x st ... we have ___" can be formalized to $\forall x (\cdots \to$ ___$)$
- statements of form "there is an x with ... st ___" can be formalized to $\exists x (\cdots \wedge$ ___$)$

Example. cardinality statments
- "there are at least two elements" is formalized
  $\phi_{\geq 2} := \exists v_0 \exists v_1 \neg v_0 \equiv v_1$
  so for all S and all S-structures $\mathfrak{A}$,
  $\mathfrak{A} \models \phi_{\geq 2}$ iff A contains at least two elements
- "there are at least n ($n \geq 3$) elements" is sentence
  $\phi_{\geq n} := \exists v_0 \cdots \exists v_n (\neg v_0 \equiv v_1 \wedge \cdots \wedge \neg v_0 \equiv v_{n-1} \wedge \cdots \wedge \neg v_{n-2} \equiv v_{n-1})$
- "there are fewer than n elements" is sentence $\neg \phi_{\geq n}$
- "there are exactly n elements" is sentence $\phi_{\geq n} \wedge \neg \phi_{\geq n+1}$
- let $\Phi_\infty := \{\phi_{\geq n} | n \geq 2\}$
  the models of Φ_∞ are precisely the infinite structures
  ie for all S and all S-structures $\mathfrak{A}$, $\mathfrak{A} \models \Phi_\infty$ iff A contains infinitely many elements

Example. theory of orderings and partial orderings
- an ordering is structure $\mathfrak{A} = (A, <^{\mathfrak{A}})$ which is a model of the sentences
  $$\Phi_{ord} \begin{cases} \forall x \neg x < x \\ \forall x \forall y \forall z ((x < y \wedge x < z) \to x < z) \\ \forall x \forall y (x < y \vee x \equiv y \vee y < x) \end{cases}$$
- ex $(\mathbb{R}, <^{\mathbb{R}})$ and $(\mathbb{N}, <^{\mathbb{N}})$ are orderings
  ex $(\mathbb{C}, <^{\mathbb{C}})$, where $z_1 <^{\mathbb{C}} z_2$ means $z_1, z_2 \in \mathbb{R}$ and $z_1 <^{\mathbb{R}} z_2$, is not an ordering since third axiom is violated
- Let structure $\mathfrak{A} = (A, <^{\mathfrak{A}})$
  define field (note field will have different meaning in next example) $<^{\mathfrak{A}} := \{a \in A |$ for some $b \in A$, $a <^{\mathfrak{A}} b$ or $b <^{\mathfrak{A}} a\}$
- ex (field $<^{\mathbb{C}}, <^{\mathbb{C}}$) is an ordering since field $<^{\mathbb{C}} = \mathbb{R}$
- partially defined ordering (sometimes "partial ordering", sometimes not) is $\mathfrak{A} = (A, <^{\mathfrak{A}})$ if (field $<^{\mathfrak{A}}, <^{\mathfrak{A}}$) is an ordering
  so partial orderings are exactly the models of
  $$\Phi_{pord} \begin{cases} \exists x \exists y x < y \\ \forall x \neg x < x \\ \forall x \forall y \forall z ((x < y \wedge y < z) \to x < z) \\ \forall x \forall y ((\exists u (x < u \vee u < x) \wedge \\ \quad \exists v (y < v \vee v < y)) \to (x < y \vee x \equiv y \vee y < x)) \end{cases}$$

Example. the theory of fields and ordered fields
- take $S_{ar} = \{+, \cdot, 0, 1\}$
  a field is a S_{ar}-structure satisfying sentences
  $$\Phi_{fd} \begin{cases} \forall x \forall y \forall z (x + y) + z \equiv x + (y + z) \\ \forall x \forall y \forall z (x \cdot y) \cdot z \equiv x \cdot (y \cdot z) \\ \forall x \exists y x + y \equiv 0 \\ \forall x \forall y x + y \equiv y + x \\ \neg 0 \equiv 1 \\ \forall x \forall y \forall z x \cdot (y + z) \equiv (x \cdot y) + (x \cdot z) \\ \forall x x + 0 \equiv x \\ \forall x x \cdot 1 \equiv x \\ \forall x (\neg x \equiv 0 \to \exists y x \cdot y \equiv 1) \\ \forall x \forall y x \cdot y \equiv y \cdot x \end{cases}$$
- ordered fields are $S_{ar}^{<}$-structures which satisfy the following sentences
  $$\Phi_{ofd} \begin{cases} \text{the sentences in } \Phi_{fd} \text{ and } \Phi_{ord} \\ \forall x \forall y \forall z (x < y \to x + z < y + z) \\ \forall x \forall y \forall z ((x < y \wedge 0 < z) \to x \cdot z < y \cdot z) \end{cases}$$

Example. graph theory and directed graph theory
- Let $S = \{R\}$ where symbol R is binary relation
  graphs and directed graphs are S-structure $\mathfrak{G} = (G, R^{\mathfrak{G}})$ are models of
  $\Phi_{dgph} := \{\forall x \neg Rxx\}$
  $\Phi_{gph} := \{\forall x \neg Rxx, \forall x \forall y (Rxy \leftrightarrow Ryx)\}$
- intuition of graphs:
  (directed) graph $\mathfrak{G} = (G, R^{\mathfrak{G}})$, $R^{\mathfrak{G}} ab$ for $a, b \in G$ means a, b are connected by a (arrow) line from a to b
  pair (a, b) is called (directed) edge of $\mathfrak{G}$ and elements of G are called vertices of $\mathfrak{G}$

3.7. SOME REMARKS ON FORMALIZABILITY.

Remark. this section: some difficulties which arise in formalization

3.7.1. *PARTIAL FUNCTIONS.*

Remark. we interpretted function symbols as total functions ie over entire domain
but sometimes not over entire domain

Example. division function over $\mathbb{R}$ undefined over 0.
Possible solutions:
- extend division function to a total function by defining $\frac{r}{0} := 0$ for all $r \in \mathbb{R}$
- instead of division function, consider its graph, the ternary relation $\{(a, b, c) \in \mathbb{R}^3 | b \neq 0, \frac{a}{b} = c\}$
  see VIII.1 for translating statements about functions to statements about their graphs
- introduce first-order languages which include partial functions
  but this creates overcomplicated logical systems

3.7.2. *MANY-SORTED FUNCTIONS.*

Remark. we interpretted domain to have elements of same *sort*
some math structures contain elements of different *sorts*

Example. vector spaces consist of vectors and scalars
possible solutions:
- many-sorted languages: let two-sorted structure (two domains):
  $\mathfrak{V} = (F, V, +^F, \cdot^F, 0^F, \circ^V, e^V, *^{F,V})$
  where field of scalars $(F, +^F, \cdot^F, 0^F)$, additive group of vectors $(V, \circ^V, e^V)$, and $*^{F,V} : F \times V \to V$
  two-sorted language has two sorts of variables, $u_0, u_1, u_2, \ldots$ for scalars and $w_0, w_1, w_2, \ldots$ for vectors
  some axioms for vector spaces:
  α) associativity of scalar addition:
  $\forall u_0 \forall u_1 \forall u_2 (u_0 + u_1) + u_2 \equiv u_0 + (u_1 + u_2)$
  β) associativity of vector addition:
  $\forall w_0 \forall w_1 \forall w_2 (w_0 \circ w_1) \circ w_2 \equiv w_0 \circ (w_1 \circ w_2)$
  γ) associativity of scalar multiplication of vectors:
  $\forall u_0 \forall u_1 \forall w_0 (u_0 \cdot u_1) * w_0 \equiv u_0 * (u_1 * w_0)$
- sort reduction
  use one set with "sort symbols" $\underline{F}, \underline{V}$ interpretted as relations $\underline{F}^{\mathfrak{V}}, \underline{V}^{\mathfrak{V}}$ $\mathfrak{V} = (F \cup V, \underline{F}^{\mathfrak{V}}, \underline{V}^{\mathfrak{V}}, +^{\mathfrak{V}}, \cdot^{\mathfrak{V}}, 0^{\mathfrak{V}}, \circ^{\mathfrak{V}}, e^{\mathfrak{V}}, *^{\mathfrak{V}})$
  some axioms:
  α) $\forall x \forall y \forall z ((\underline{F}x \wedge \underline{F}y) \wedge \underline{F}z) \to (x + y) + z \equiv x + (y + z))$
  β) $\forall x \forall y \forall z ((\underline{V}x \wedge \underline{V}y) \wedge \underline{V}z) \to (x \circ y) \circ z \equiv x \circ (y \circ z))$
  γ) $\forall x \forall y \forall z ((\underline{F}x \wedge \underline{F}y) \wedge \underline{V}z) \to (x \cdot y) * z \equiv x * (y * z))$
  note: $+^{\mathfrak{V}}, \cdot^{\mathfrak{V}}, \circ^{\mathfrak{V}}, *^{\mathfrak{V}}$ are extended to $(F \cup V) \times (F \cup V) \mapsto (F \cup V)$ arbitrarily

3.7.3. *LIMITS OF FORMALIZABILITY.*

Remark. will discuss two examples, see VI and VII.2 for more

Example.
- Torsion groups.
  torsion group $\mathfrak{G}$ is group st every element has finite order ie for each $a \in G$, $a^n = e^G$ for $n \in \mathbb{N}$ formally,
  $\forall x (x \equiv e \vee x \circ x \equiv e \vee (x \circ x) \circ x \equiv e \vee \ldots)$
  But first-order formula does not allow infinitely long disjunction
  will see later that there is no set of first-order formulas whose models are precisely the torsion groups
- Peano's Axoims.
  following results can extend to S_{ar}-structure $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$ (ex 7.5)
  consider structure $\mathfrak{N}_\sigma = (\mathbb{N}, \sigma, 0)$ where σ is successor function.
  $\mathfrak{N}_\sigma$ satisfies Peano axioms

α) 0 is not a value of σ
β) σ is injective
γ) (induction axiom) for every subset $X \subset \mathbb{N}$, if $0 \in X$ and if $\sigma(n) \in X$ for $n \in X$ then $X = \mathbb{N}$
Formulate α, β as $L^{\{\sigma,0\}}$ sentences, and γ as a second-order formula (cf IX.1)
(P1) $\forall x \neg \sigma x \equiv 0$
(P2) $\forall x \forall y (\sigma x \equiv \sigma y) \to x \equiv y$
(P3) $\forall X((X0 \wedge \forall x(Xx \to X\sigma x)) \to \forall y Xy)$
following thm shows that (P1),(P2),(P3) characterize $\mathfrak{N}_\sigma$ up to isomorphism

Theorem. *(7.4)(Dedekind's thm)*
every structure $\mathfrak{A} = (A, \sigma^A, 0^A)$ which satisfies (P1),(P2),(P3) is isomorphic to $\mathfrak{N}_\sigma$

Proof. Assume $\mathfrak{A}$ satisfies (P1),(P2),(P3).
since $\mathfrak{A}$ satisfies (P3), can give *proof by induction in* $\mathfrak{A}$
see book for proof of isomorphism $\pi : \mathfrak{A} \cong \mathfrak{N}_\sigma$

Remark. VI.4: no set of first-order $\{\sigma, 0\}$-sentences has just $\mathfrak{N}_\sigma$ (and its isomorphisms) as a model. Thus the induction axiom cannot be formalized in the first-order language $L^{\{\sigma,0\}}$

3.8. SUBSTITUTION.

Remark.
- given formula ϕ, want to substitute a term t for variable x at places where x occurs free in ϕ
- want new formula to express the same about t as ϕ does about x

Example. special care is needed
$\phi := \exists z z + z = x$
replace x by z: $\exists z z + z = z$
The meaning changes since substituted z gets bound.
instead, should modify ϕ to $\exists u u + u = x$ and then substitute z for x, where u is distinct from z, x

Definition. Let S, let pairwise distinct variables $x_0, \dots, x_r$ and arbitrary terms $t_0, \dots, t_r$. Define $\phi \frac{t_0 \dots t_r}{x_0 \dots x_r}$ as simultaneous substitution of $t_0, \dots, t_r$ for $x_0, \dots, x_r$ st
- by induction on terms
  $x \frac{t_0 \dots t_r}{x_0 \dots x_r} := \begin{cases} x & \text{if } x \neq x_0, \dots, x \neq x_r \\ t_i & \text{if } x = x_i \end{cases}$
  $c \frac{t_0 \dots t_r}{x_0 \dots x_r} := c$
  $[f t'_1 \dots t'_n] \frac{t_0 \dots t_r}{x_0 \dots x_r} := f t'_1 \frac{t_0 \dots t_r}{x_0 \dots x_r} \dots t'_n \frac{t_0 \dots t_r}{x_0 \dots x_r}$
- by induction on formulas
  $[t'_1 \equiv t'_2] \frac{t_0 \dots t_r}{x_0 \dots x_r} := t'_1 \frac{t_0 \dots t_r}{x_0 \dots x_r} \equiv t'_2 \frac{t_0 \dots t_r}{x_0 \dots x_r}$
  $[R t'_1 \dots t'_n] \frac{t_0 \dots t_r}{x_0 \dots x_r} := R t'_1 \frac{t_0 \dots t_r}{x_0 \dots x_r} \dots t'_n \frac{t_0 \dots t_r}{x_0 \dots x_r}$
  $[\neg \phi] \frac{t_0 \dots t_r}{x_0 \dots x_r} := \neg [\phi \frac{t_0 \dots t_r}{x_0 \dots x_r}]$
  $(\phi \vee \psi) \frac{t_0 \dots t_r}{x_0 \dots x_r} := \phi \frac{t_0 \dots t_r}{x_0 \dots x_r} \vee \psi \frac{t_0 \dots t_r}{x_0 \dots x_r}$
  $[\exists x \phi] \frac{t_0 \dots t_r}{x_0 \dots x_r} := \exists u [\phi \frac{t_{i_1} \dots t_{i_s} u}{x_{i_1} \dots x_{i_s} x}]$
  where $x_{i_1}, \dots, x_{i_s}$, $i_1 < \dots < i_s$, are exactly the variables among $x_0, \dots, x_r$ st $x_i \in \text{free}(\phi)$ and $x_i \neq t_i$
  where $u = \begin{cases} x & \text{if } x \text{ not occur in } t_{i_1}, \dots, t_{i_s} \\ \text{"fresh"} & \text{o.w.; fresh is first var not in } \phi, t_{i_1}, \dots, t_{i_s} \end{cases}$

Remark.
- we made sure no variable occuring in $t_{i_1}, \dots, t_{i_s}$ falls under the scope of a quantifier
- case there is no x_i st $x_i \in \text{free}(\exists x \phi)$ and $x_i \neq t_i$ then $[\exists x \phi] \frac{t_0 \dots t_r}{x_0 \dots x_r} = \exists x [\phi \frac{x}{x}]$ (which equals $\exists x \phi$ by lem 8.4)

Example. let P binary rel, f binary func
- $[P v_0 f v_1 v_2] \frac{v_2 v_0 v_1}{v_1 v_2 v_3} = P v_0 f v_2 v_0$
- $[\exists v_0 P v_0 f v_1 v_2] \frac{v_4\ f v_1 v_1}{v_0\ v_2} = \exists v_0 [[P v_0 f v_1 v_2] \frac{f v_1 v_1\ v_0}{v_2\ v_0}]$
  $= \exists v_0 P v_0 f v_1 f v_1 v_1$
- $[\exists v_0 P v_0 f v_1 v_2] \frac{v_0 v_2 v_4}{v_1 v_2 v_0} = \exists v_3 [[P v_0 v_1 v_2] \frac{f v_0 v_3}{v_1 v_0}]$
  $= \exists v_3 P v_3 f v_0 v_2$

Remark. how about interpretation before and after substitution

Definition. let $\mathfrak{I} = (\mathfrak{A}, \beta)$; $x_0, \dots, x_r$ pairwise distinct, $a_0, \dots, a_r \in A$.
define $\beta \frac{a_0 \dots a_r}{x_0 \dots x_r}(y) := \begin{cases} \beta(y) & \text{if } y \neq x_0, \dots, y \neq x_r \\ a_i & \text{if } y = x_i \end{cases}$
define $\mathfrak{I} \frac{a_0 \dots a_r}{x_0 \dots x_r} := (\mathfrak{A}, \beta \frac{a_0 \dots a_r}{x_0 \dots x_r})$

Lemma. *(substitution lemma)*
a) for every term t, $\mathfrak{I}\left(t \frac{t_0 \dots t_r}{x_0 \dots x_r}\right) = \mathfrak{I} \frac{\mathfrak{I}(t_0) \dots \mathfrak{I}(t_r)}{x_0 \dots x_r}(t)$
b) for every formula ϕ,
$\mathfrak{I} \models \phi \frac{t_0 \dots t_r}{x_0 \dots x_r}$ iff $\mathfrak{I} \frac{\mathfrak{I}(t_0) \dots \mathfrak{I}(t_r)}{x_0 \dots x_r} \models \phi$

Proof. induction on terms, induction on formulas see book

Remark.
- . [intuition: substitution lemma allows moving stuff between formal domain and real-world math domain, so can do normal mathematics on it]
- the following lemmas are several "syntactic" properties of substitution

Lemma. *(8.4)*
a) for every permutaion π of the numbers $0, \dots, r$,
$\phi \frac{t_0 \dots t_r}{x_0 \dots x_r} = \phi \frac{t_{\pi(0)} \cdots t_{\pi(r)}}{x_{\pi(0)} \cdots x_{\pi(r)}}$
b) if $0 \leq i \leq r$ and $x_i = t_i$, then
$\phi \frac{t_0 \dots t_r}{x_0 \dots x_r} = \phi \frac{t_0 \dots t_{i-1} t_{i+1} \dots t_r}{x_0 \dots x_{i-1} x_{i+1} \dots x_r}$
in particular, $\phi \frac{x}{x} = \phi$
c) for every variable y,
i) if $y \in var\left(t \frac{t_0 \dots t_r}{x_0 \dots x_r}\right)$
then $(y \in var(t_0) \cup \dots \cup var(t_r))$ or $(y \neq x_0, \dots, y \neq x_r)$
ii) if $y \in free\left(\phi \frac{t_0 \dots t_r}{x_0 \dots x_r}\right)$
then $(y \in var(t_0) \cup \dots \cup var(t_r))$ or $(y \in free(\phi)$ and $y \neq x_0, \dots, y \neq x_r)$

Proof. induction, use defs, see book for some cases of (c)

Corollary. *(8.5)*
Let $free(\phi) \subset \{x_0, \dots, x_r\}$
continue assuming $x_0, \dots, x_r$ distinct
if terms $t_0, \dots, t_r$ st $var(t_i) \subset \{v_0, \dots, v_r\}$
then formula $\phi \frac{t_0 \dots t_r}{x_0 \dots x_r}$ is in L_n^S
in particular, $\phi \frac{a_0 \dots a_r}{x_0 \dots x_r}$ is a sentence

Definition. the rank of ϕ, $\text{rk}(\phi)$, is its number of connectives and quantifiers.
by induction on formulas:
$\text{rk}(\phi) := 0$ if ϕ atomic
$\text{rk}(\neg\phi) :=\text{rk}(\phi) + 1$
$\text{rk}(\phi \vee \psi) :=\text{rk}(\phi)+\text{rk}(\psi) + 1$
$\text{rk}(\exists x \phi) :=\text{rk}(\phi) + 1$
$\text{rk}(\phi \frac{t_0 \dots t_r}{x_0 \dots x_r}) :=\text{rk}(\phi)$

Proof. immediate from def of substitution

Remark.
- can formulate "there exists exactly one x st ϕ"
  Let y the first variable different from x and does not occur free in ϕ
  $\exists x(\phi \wedge \forall y(\phi \frac{y}{x} \to x \equiv y))$
- notation: $\exists^{=1} x \phi$
- can show for every $\mathfrak{I}$:
  $\mathfrak{I} \models \exists^{=1} x \phi$ iff there is exactly one $a \in A$ st $\mathfrak{I} \frac{a}{x} \models \phi$

4. A SEQUENT CALCULUS

Remark. a mathematical theory is developed by finding which propositions follow from its axioms, using proofs

Definition.
- $\Phi^\models$ is set of S-sentences which are consequences of the set Φ of S-sentences
- mathematical proof of S-sentence ϕ from axioms in Φ shows that ϕ belongs to $\Phi^\models$

Example. Let Φ_{gr}, S_{gr}.
Proof of 1.1.1 showed that $\forall x \exists y y \circ x \equiv e$ belongs to $\Phi_{gr}^\models$

Remark.
- can every sentence in $\Phi^\models$ be proved from the axioms in Φ?
  need to analyze the notion of proof
- mathematicians often do not have an exact notion of proof from a list of permissible inferences only acquantance by doing proofs
- the collection of commonly accepted methods of proof continually expands with new variants
- new theories often include new proof techniques
- will look at some basic mathematical arguments (deductions) which turn out to be sufficient to reconstruct all types of mathematical arguments
- will use first order language to give a precise notion of proof
- limited expressive power of first order languages are plausibly sufficient for mathematics (cf VIII.2)
  but can prove that every sentence in $\Phi^\models$ is provable from sentences in Φ

Example. from pfs in ch1, some basic mathematical deduction schemes are
$\frac{\phi, \psi}{(\phi \wedge \psi)}$, $\frac{Pt}{\exists x P x}$, $\frac{P x, x \equiv t}{Pt}$
constituents of pfs are regarded as syntactic operations of symbol strings
ie can proceed from top to bottom

Remark.
- this chapter:
  §1: motivation for form of calculus
  §2,4: calculus $\mathfrak{G}$
  §6: definition of a formula ϕ being formally provable from a set Φ of formulas, based on derivability in $\mathfrak{G}$
- formal provability is the syntactic couterpart to semantic notion of consequence
- throughout ch4, fix symbol set S

4.1. SEQUENT RULES.

Remark.
- mathematical proof of a thm is a list of statements: hypothesis, ..., thm
- can temporarily assume additional hypotheses eg to prove intermediate claim ϕ by contradiction, if a contradition results, then ϕ has been proved, and the additional assumption $\neg\phi$ can be dropped
- each stage of pf is list of assumptions and the claim

Definition. sequent is a nonempty sequence ("list") of formulas

Remark.
- sequents describe stages of pf
- ntn: assumptions $\phi_1, ..., \phi_n$ and claim ϕ is rendered by sequent $\phi_1 ... \phi_n \phi$

Definition. Let sequent $\phi_1 ... \phi_n \phi$.
$\phi_1 ... \phi_n$ is antecedent and ϕ is succedent
ntn: use Γ to denote (possibly empty) antecedent $\phi_1 ... \phi_n$

Claim. *formulas which constitute a sequent are uniquely determined*
in particular, the antecedent and succedent are well defined

Proof. unique readability

Example. schematic of indirect pf above

Γ	$\neg\phi$	ψ	
Γ	$\neg\phi$	$\neg\psi$	is read "if under assumptions Γ(=
Γ		ϕ	

$\phi_1, ..., \phi_n$) one can obtain both formla ψ and $\neg\psi$ (a contradiction), then from the assumptions Γ one can infer ϕ"
ntn: spaces allow easier reading

Remark. "deduction rules" of "sequent calculus" $\mathfrak{G}$ operate on sequents
ie each stage ("step") of a pf passes already attained sequents to a new sequent

Definition.
- sequent $\Gamma\phi$ is defivable, "$\vdash \Gamma\phi$", in calculus $\mathfrak{G}$ means there is a derivation of $\Gamma\phi$
- formula ϕ is formally provable ("derivable") from a set Φ of formulas, "$\Phi \vdash \phi$", means there are finitely many $\phi_1, ...\phi_n \in \Phi$ st $\vdash \phi_1 ... \phi_n \phi$
- sequent $\Gamma\phi$ is correct, "$\Gamma \models \phi$", means $\{\psi : \psi$ is a member of $\Gamma\} \models \phi$
- correct rules are rules of $\mathfrak{G}$ st when applied to correct sequents yield a correct sequent

Remark. we will use correct rules

Claim. *every formula derivable from Φ (using correct rules) also follows from Φ*
ie if $\Phi \vdash \phi$ then $\Phi \models \phi$

4.2. STRUCTURAL RULES AND CONNECTIVE RULES.

Remark.
- categories of rules of the sequent calculus:
  structural rules (2.1,2.2)
  connective rules (2.3,2.4,2.5,2.6)
  quantifier rules (4.1,4.2)
  equality rules (4.3,4.4)
- see book for correcness proofs

Definition.
- Antecedent rule (Ant)
  $\dfrac{\Gamma \quad \phi}{\Gamma' \quad \phi}$ if every member of Γ is also a member of Γ' ("$\Gamma \subset \Gamma'$")
  note: a formula which occurs more than once in Γ need only occur once in Γ'
  intuition: can reorder or add to assumptions
- Assumption rule (Assm)
  $\dfrac{}{\Gamma \quad \phi}$ if ϕ is a member of Γ
  intuition: can conclude ϕ from a set of assumptions which includes ϕ
- Proof by cases (PC)
  $\dfrac{\Gamma \quad \psi \quad \phi \qquad \Gamma \quad \neg\psi \quad \phi}{\Gamma \quad \phi}$
  intuition: to conclude ϕ from Γ, first consider cases where ψ and then $\neg\psi$ are additional assumptions
- Contradiction rule (Ctr)
  $\dfrac{\Gamma \quad \neg\phi \quad \psi \qquad \Gamma \quad \neg\phi \quad \neg\psi}{\Gamma \quad \phi}$
- $\vee$ rule for the antecedent ($\vee$A)
  $\dfrac{\Gamma \quad \phi \quad \chi \qquad \Gamma \quad \psi \quad \chi}{\Gamma \quad (\phi \vee \psi) \quad \chi}$
- $\vee$ rule for the succedeedent ($\vee$S)
  a) $\dfrac{\Gamma \quad \phi}{\Gamma \quad (\phi \vee \psi)}$ b) $\dfrac{\Gamma \quad \phi}{\Gamma \quad (\psi \vee \phi)}$

4.3. DERIVABLE CONNECTIVE RULES.

Remark. can derive rules with just the following rules of $\mathfrak{G}$: Ant, Assm, PC, Ctr, $\vee$A, $\vee$S x

Claim. *Tertium non duter (TND)*

$\dfrac{}{(\phi \vee \neg\phi)}$
intuition: all sequents of the form $(\phi \vee \neg\phi)$ are derivable

Proof. Justification: use rules from $\mathfrak{G}$ to go from premise sequents to sequent

1.	ϕ	ϕ	(Assm)
2.	ϕ	$(\phi \vee \neg\phi)$	($\vee$S) to 1
3.	$\neg\phi$	$\neg\phi$	(Assm)
4.	$\neg\phi$	$(\phi \vee \neg\phi)$	($\vee$S) to 3
5.		$(\phi \vee \neg\phi)$	(PC) to 2,4

note: ntn similar to derivation in calc of terms and calc of formulas

Remark.
- adding TND to $\mathfrak{G}$ does not enlarge the set of derivable sequents
- in a derivation of a sequent using $\mathfrak{G}$ and TND, can put lines 1-4 directly before $(\phi \vee \neg\phi)$ to get derivation using only rules in $\mathfrak{G}$
- derivable rules like TND allow shorter derivations in the sequent calculus
- see book for justification of the following derived rules

Claim.
- *Second contradiction rule (Ctr')*
  $\dfrac{\Gamma \quad \psi \qquad \Gamma \quad \neg\psi}{\Gamma \quad \phi}$
- *Chain rule (Ch)*
  $\dfrac{\Gamma \quad \phi \qquad \Gamma \quad \phi \quad \psi}{\Gamma \quad \psi}$
- *Contraposition rule (Cp)*
  a) $\dfrac{\Gamma \quad \phi \quad \psi}{\Gamma \quad \neg\psi \quad \neg\phi}$ *b)* $\dfrac{\Gamma \quad \neg\phi \quad \neg\psi}{\Gamma \quad \psi \quad \phi}$
  c) $\dfrac{\Gamma \quad \neg\phi \quad \psi}{\Gamma \quad \neg\psi \quad \phi}$ *d)* $\dfrac{\Gamma \quad \phi \quad \neg\psi}{\Gamma \quad \psi \quad \neg\phi}$
- *noname*
  $\dfrac{\Gamma \quad (\phi \vee \psi) \qquad \Gamma \quad \neg\phi}{\Gamma \quad \psi}$
- *Modus ponens*
  $\dfrac{\Gamma \quad (\phi \to \psi) \qquad \Gamma \quad \phi}{\Gamma \quad \psi}$ *ie* $\dfrac{\Gamma \quad (\neg\phi \vee \psi) \qquad \Gamma \quad \phi}{\Gamma \quad \psi}$

4.4. QUANTIFIER AND EQUALITY RULES.

Remark. see book for correctness of following four rules

Definition.
- Rule for $\exists$-introduction in the succedent ($\exists$S)
  $\dfrac{\Gamma \quad \phi\frac{t}{x}}{\Gamma \quad \exists x\phi}$
  intuition: can conclude $\exists x\phi$ from Γ if we have already obtained a "witness" t for this existence claim

Remark.
- next rule incorporates frequently used method of argument
- want to prove claim ψ from assumptions $\phi_1, ..., \phi_n, \exists x\phi$
  formally, want to derive sequent $\phi_1 ... \phi_n \exists x\phi\psi$
- from hypothesis $\exists x\phi$, assume example y, a new variable, "satisfies" ϕ and use it to prove ψ
  formally, this is derivation of $\phi_1 ... \phi_n \phi\frac{y}{x}\psi$ where y not free in $\phi_1 ... \phi_n \exists x\phi\psi$

Definition. Rule for $\exists$-introduction in the antecedent ($\exists$A)
$\dfrac{\Gamma \quad \phi\frac{y}{x} \quad \psi}{\Gamma \quad \exists x\phi \quad \psi}$ if y not free in $\Gamma \exists x\phi\psi$

Example. the condition on y is essential
- sequent $[x \equiv fy]\frac{y}{x}\ y \equiv fy$ is correct
- sequent $\exists x x \equiv fy\ y \equiv fy$ is not correct since interpretation $\mathbb{N}$, f is successor function and y is 0

Remark.
cant, in general, recover ϕ or t from $\phi\frac{t}{x}$
eg Rfy can be written $Rx\frac{fy}{x}$ or $Rfx\frac{y}{x}$
so when applying ($\exists$S) and ($\exists$A), will explicitly mention ϕ and t or ϕ and y if they are not clear

Definition.
- Reflexivity rule for equality ($\equiv$)
  $\dfrac{}{t \equiv t}$
- Substitution rule for equality ($\equiv$)
  $\dfrac{\Gamma \qquad \phi\frac{t}{x}}{\Gamma \quad t \equiv t' \quad \phi\frac{t'}{x}}$

4.5. FURTHER DERIVABLE RULES AND SEQUENTS.

Remark. see book for justification of the following derived rules

Claim.
- *special case of ($\exists$S) with $t \equiv x$ (note $\phi\frac{x}{x} = \phi$)*
  $\dfrac{\Gamma \quad \phi}{\Gamma \quad \exists x\phi}$
- *special case of ($\exists$A) with $y \equiv x$*
  $\dfrac{\Gamma \quad \phi \quad \psi}{\Gamma \quad \exists x\phi \quad \psi}$
- *special case of (Sub)* $\dfrac{\Gamma \qquad \phi}{\Gamma \quad x \equiv t \quad \phi\frac{t}{x}}$
- *Symmetry of equality* $\dfrac{\Gamma \quad t_1 \equiv t_2}{\Gamma \quad t_2 \equiv t_1}$
- *Transitivity of equality* $\dfrac{\Gamma \quad t_1 \equiv t_2 \qquad \Gamma \quad t_2 \equiv t_3}{\Gamma \quad t_1 \equiv t_3}$
- *Compatibility of equality with functions and relations*
  a) $\dfrac{\Gamma \quad Rt_1 ... t_2 \qquad \Gamma \quad t_1 \equiv t_1' \qquad \vdots \qquad \Gamma \quad t_n \equiv t_n'}{\Gamma \quad Rt_1' ... t_n'}$
  b) $\dfrac{\Gamma \qquad t_1 \equiv t_1' \qquad \vdots \qquad \Gamma \qquad t_n \equiv t_n'}{\Gamma \quad ft_1 ... t_2 \equiv ft_1' ... t_n'}$

4.6. SUMMARY AND EXAMPLE.

Lemma. *For all Φ and ϕ*
$\Phi \vdash \phi$ iff there is a finite subset Φ_0 of Φ st $\Phi_0 \vdash \phi$

Proof. recall $\Phi \vdash \phi$ if there are formulas $\phi_1, ..., \phi_n \in \Phi$ st $\vdash \phi_1 ... \phi_n \phi$

Theorem. *(Correctness of $\mathfrak{G}$)*
For all Φ and ϕ, if $\Phi \vdash \phi$ then $\Phi \models \phi$

Proof. by induction over $\mathfrak{G}$
every rule without premises yields a correct sequence
other rules always yield correct sequents from correct sequents

Remark.
- above thm's converse ($\Phi \models \phi \Rightarrow \Phi \vdash \phi$) will be proved in ch 5
  intuition: if ϕ is mathematically provable from Φ ($\Phi \models \phi$) then ϕ is also formally provable from Φ
- formal proof is more elementary in character so can be long
  see book for formal pf of existence of left inverse from group axioms

4.7. CONSISTENCY.

Remark. corresponding concepts:

syntactic	semantic
consequence ($\models$)	derivability ($\vdash$)
satisfiability (Sat)	consistency (Con)

Definition.
- $\Phi \subset L^S$ is consistent, ConΦ, means there is no formula ϕ st $\Phi \vdash \phi$ and $\Phi \vdash \neg\phi$
- Φ is inconsistent, IncΦ, means there is such a formula

Lemma. *(7.3) Let set Φ of formulas*
IncΦ $\Leftrightarrow$ for all formulas ϕ, $\Phi \vdash \phi$

Corollary. *(7.3)*
Let set Φ of formulas
*ConΦ $\Leftrightarrow$ there is a formula ϕ which is **not** derivable from Φ*

Lemma. *(7.4)*
For all Φ, ConΦ iff ConΦ_0 for all finite subsets Φ_0 of Φ

Proof. $\Phi \vdash \phi$ iff $\Phi_0 \vdash \phi$ for a suitable finite subset Φ_0 of Φ

Lemma. *(7.5)*
Every satisfiable set of formulas is consistent

Proof. book, short

Lemma. *(7.6)*
For all Φ and ϕ with ConΦ, the following holds
a) $\Phi \vdash \phi$ iff Inc$\Phi \cup \{\neg\phi\}$
b) $\Phi \vdash \neg\phi$ iff Inc$\Phi \cup \{\phi\}$
c) Con$\Phi \cup \{\phi\}$ or Con$\Phi \cup \{\neg\phi\}$

Proof. book

Remark.
- notation if using multiple symbol sets simultaneously
  $\mathfrak{G}_S$, $\vdash_S$, Con_S
- will show later that for $S \subset S'$, $\Phi \subset L^S$, $\phi \in L^S$ can't have $\Phi \vdash_{S'} \phi$ but not $\Phi \vdash_S \phi$
  see book for intuition
- following lem needed for next chapter

Lemma. *(7.7)*
For $n \in \mathbb{N}$, let S_n be symbol sets st $S_0 \subset S_1 \subset S_n \subset ...$
Let Φ_n be sets of S_n-formulas st Con$_{S_n}\Phi_n$ and $\Phi_0 \subset \Phi_1 \subset \Phi_2 \subset ...$
Let $S = \cup_{n\in\mathbb{N}} S_n$ and $\Phi = \cup_{n\in\mathbb{N}}\Phi_n$
Then Con$_S\Phi$

Proof. book

5. THE COMPLETENESS THM

Remark. this chapter
- big clm: every consistent set of formulas is satisfiable
  pf: will have to find a model for any given consistent set Φ of formulas
  §1: for Φ is negation complete and contains witnesses
  §2: reduce general case to at most ctble symbol sets
  §3: arbitrary symbol sets
- completeness thm: $\Phi \models \phi \Rightarrow \Phi \vdash \phi$
  pf: towards contradiction, assume $\Phi \models \phi \Rightarrow$ not $\Phi \vdash \phi$
  then $\Phi \cup \{\neg\phi\}$ is consistent (7.6b) and not satisfiable (III.4.4)
  contradiction, since above big clm
- will fix S unless otherwise stated

5.1. HENKIN'S THEOREM.

Remark.
- given consistent set of formulas Φ
  want to find an interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ satisfying Φ
- can only use consistency (which is syntactic)

Remark. naive attempt
- take domain $A := T^S$, the set of all S-terms
  define $\beta(v_i) := v_i$ for $i \in \mathbb{N}$
  interpret function symbol f (eg unary) by $f^{\mathfrak{A}}(t) := ft$
  interpret relation symbol R (eg unary) by $R^{\mathfrak{A}}(t) := \{t \in A : \phi \vdash Rt\}$
  eg for a variable x, $\mathfrak{I}(fx) = f^{\mathfrak{A}}(\beta(x)) = fx$
- difficulty: if variable y is different from x then $fx \neq fy$ hence $\mathfrak{I}(fx) \neq \mathfrak{I}(fy)$
  eg $\Phi = \{fx \equiv fy\}$
  ie $\mathfrak{I}$ would not be a model of Φ
  see book for more details
- solution to difficulty: define an equivalence relation on terms and use equivalence classes as elemetns of domain of $\mathfrak{I}$
- the following is towards the definition of $\mathfrak{I}^\Phi = (\mathfrak{A}^\Phi, \beta^\Phi)$

Definition. binary relation $\sim$ on the set T^S of S-terms by
$t_1 \sim t_2$ iff $\Phi \vdash t_1 \equiv t_2$

Lemma.
a) $\sim$ is an equivalence relation
b) $\sim$ is compatible with the symbols in S in the following sense:
if $t_1 \sim t_1', ..., t_n \sim t_n'$
then for every n-ary $f \in S$, $ft_1...t_n \sim ft_1'...t_n'$
and for every n-ary $R \in S$, $\Phi \vdash Rt_1...t_n$ iff $\Phi \vdash Rt_1'...t_n'$

Proof. book

Definition.
- $\overline{t} := \{t \in T^S : t \sim t'\}$ ie equivalence class of t
- $T^{\Phi,S} := \{\overline{t} : t \in T^S\}$ ie the set of equivalence classes
  ntn: T^Φ
  note: nonempty
- the term structure $\mathfrak{T}^\Phi$ over T^Φ is st
  for n-ary $R \in S$, $R^{\mathfrak{T}^\Phi}\overline{t}_1, ..., \overline{t}_n$:iff $\Phi \vdash Rt_1...t_n$
  for n-ary $f \in S$, $f^{\mathfrak{T}^\Phi}(\overline{t}_1, ..., \overline{t}_n) := \overline{ft_1...t_n}$
  for $c \in S$, $c^{\mathfrak{T}^\Phi} := \overline{c}$

Claim. *$R^{\mathfrak{T}^\Phi}$ and $f^{\mathfrak{T}^\Phi}$ are well-defined*

Proof. defs are indep of choice of representatives $t_1, ..., t_n$ of $\overline{t}_1, ..., \overline{t}_n$
since most recent lemma (b)

Definition.
- assignment $\beta^\Phi(x) := \overline{x}$
- term interpretation associated with Φ is $\mathfrak{I}^\Phi := (\mathfrak{A}^\Phi, \beta^\Phi)$

Lemma. *(1.7)*
a) for all t, $\mathfrak{I}^\Phi(t) = \overline{t}$
b) for every atomic formula ϕ,
$\mathfrak{I}^\Phi \models \phi$ iff $\mathfrak{I}^\Phi \vdash \phi$
c) for every formula ϕ and pairwise distinct variables $x_1, ..., x_n$,
i) $\mathfrak{I}^\Phi \models \exists x_1...\exists x_n\phi$ iff there are $t_1, ..., t_n \in T^S$ with $\mathfrak{I}^\Phi \models \phi\frac{t_1...t_n}{x_1...x_n}$
ii) $\mathfrak{I}^\Phi \models \forall x_1...\exists x_n\phi$ iff for all $t_1, ..., t_n \in T^S$ with $\mathfrak{I}^\Phi \models \phi\frac{t_1...t_n}{x_1...x_n}$

Proof. book

Remark.
- lem (b) $\Rightarrow \mathfrak{I}^\Phi$ models atomic ϕ.
- but for general ϕ, it is not true that $\mathfrak{I}^\Phi \models \phi \Rightarrow \Phi \vdash \phi$
  pf: eg $S = \{R\}$, $\Phi = \{\exists xRx\}$
  lem(c) $\Rightarrow$ if $\mathfrak{I}^\Phi \models \Phi$ then there should be t st $\exists xRx \vdash Rt$ (in our case, $t =$ variable y)
  this can easily be refuted (also see ex 1.12)
- to show $\mathfrak{I}^\Phi \models \Phi$, need Φ to satisfy two closure conditions

Definition.
- Φ contains witnesses iff for every formula of form $\exists x\phi$, there is a term t st $\Phi \vdash (\exists x\phi \to \phi\frac{t}{x})$
- Φ negation complete iff for every formula ϕ, $\Phi \vdash \phi$ or $\Phi \vdash \neg\phi$

Lemma. *(1.9)*
Let Φ consitent, neg complete, contains witnesses then for all ϕ and ψ
a) $\Phi \vdash \neg\phi$ iff not $\Phi \vdash \phi$
b) $\Phi \vdash (\phi \vee \psi)$ iff $\Phi \vdash \phi$ or $\Phi \vdash \psi$
c) $\Phi \vdash \exists x\phi$ iff there is a term t with $\Phi \vdash \phi\frac{t}{x}$

Proof. book

Theorem. *(1.10)(Henkin's thm)*
Let Φ consistent, neg complete, contains witnesses then for all ϕ, $\mathfrak{I}^\Phi \models \phi$ iff $\Phi \vdash \phi$

Proof. induction on the # of connectives and quantifiers in ϕ
case ϕ atomic: two lemmas ago
case $\phi = \neg\psi$: $\mathfrak{I}^\Phi \models \neg\psi$ iff not $\mathfrak{I}^\Phi \models \psi$
  iff not $\Phi \vdash \psi$ by induction hypothesis
  iff $\Phi \vdash \neg\phi$ by lem 1.9a
case $\phi = (\psi \vee \chi)$: $\mathfrak{I}^P hi \models (\psi \vee \chi)$ iff $\mathfrak{I}^\Phi \models \psi$ or $\mathfrak{I}^\Phi \models \chi$
  iff not $\Phi \vdash \psi$ or $\Phi \vdash \chi$ by induction hypothesis
  iff $\Phi \vdash (\psi \vee \chi)$ by lem 1.9b
case $\phi = \exists x\psi$: iff there is t st $\mathfrak{I}^\Phi \models \phi\frac{t}{x}$ by lem 1.7a
  iff there is t st $\Phi \vdash \phi\frac{t}{x}$ by induction
  iff $\Phi \vdash \exists x\psi$

Corollary. *in particular, $\mathfrak{I}^\Phi \models \Phi$ (ie Φ is satisfiable)*

5.2. SATISFIABILITY OF CONSISTENT SETS OF FORMULAS (THE COUNTABLE CASE).

Remark.
- last section: Φ con, neg cmplt, cnts wtnss $\Rightarrow$ sat
- this section: Φ cont, S at most ctble $\Rightarrow$ sat
  need two lemmas first which extend Φ to be consistent, neg cmplt, cnts witnesses

Lemma. *(2.1)*
Let $\Phi \subset L^S$ be consistent and let free(Φ) finite
Then there is a consistent, contains witnesses set $\Psi \in L^S$ st $\Phi \subset \Psi$

Proof. add formula $(\exists x\phi \to \phi\frac{y}{x})$ with a "new" variable y for each formula of the form $\exists x\phi$

Lemma. *(2.2)*
Let $\Phi \subset L^S$ be consistent
Then there is a consistent, neg complete set $\Theta \subset L^S$ with $\Psi \subset \Theta$

Remark. the following cor summarizes how we use the above two lems

Corollary. *(2.3)*
Let Φ consistent and free(Φ) finite
then Φ is satisfiable

Proof. Φ is extended to Ψ and then to Θ.
Θ is consistent and neg cmplt, and also cnts witnss since Ψ does already
So Θ is satisfiable by Henkin
So Φ is satisfiable since $\Phi \subset \Theta$

Remark. now drop the assumption that free(Φ) finite

Theorem. *(2.4)*
If S is at most ctble and $\Phi \subset L^S$ is consistent then Φ is satisfiable

Proof. will substitute new consts for free variables of Φ, invoke many previous results, including invoke (2.3) twice to jump to semantic domain where most of the work is done.
define $S' := S \cup \{c_0, c_1, ...\}$ where distinct $c_0, c_1, ... \notin S$.
define for $\phi \in L^S$, $n(\phi)$:=smallest m with free(ϕ) $\in \{v_0, ..., v_{m-1}\}$

Define $\phi' := \phi\frac{c_0\dots c_{n(\phi)-1}}{v_0\dots v_{n(\phi)-1}}$ and $\Phi' := \{\phi' | \phi \in \Phi\}$
note $\Phi' \subset L_0^{S'}$
- Clm: $\text{Con}_{S'}\Phi'$
  Pf: Will show every finite subset of Φ is Sat.
  Let subsets $\Phi_0 := \{\phi_1, ..., \phi_n\} \subset \Phi$ and $\Phi_0' := \{\phi_1', ..., \phi_n'\} \subset \Phi'$.
  Note $\text{Con}_S\Phi_0$ since $\text{Con}_S\Phi$ and (IV.7.4).
  So $\text{Sat}\Phi_0$ by (2.3)
  Choose $\mathfrak{I} = (\mathfrak{A}, \beta)$ st $\mathfrak{I} \models \Phi_0$
  Expand $\mathfrak{A}$ to S'-structure $\mathfrak{A}'$ with $c_i^{\mathfrak{A}'} = \mathfrak{I}(v_i)$ for $i \in \mathbb{N}$.
  Define S'-interpretation $\mathfrak{I}' = \{\mathfrak{A}', \beta\}$
  then for $\phi \in \Phi$, substitution lemma $\Rightarrow \mathfrak{I} \models \phi$ iff $\mathfrak{I}' \models \phi\frac{c_0\dots c_{n(\phi)-1}}{v_0\dots v_{n(\phi)-1}}$.
  So $\mathfrak{I} \models \Phi_0$ iff $\mathfrak{I}' \models \Phi_0'$
  So $\text{Sat}\Phi_0'$.
  So $\text{Con}_{S'}\Phi_0'$ by (IV.7.5)
  So $\text{Con}_{S'}\Phi'$ by (IV.7.4)

$\text{Sat}\Phi'$ since $\text{Con}_{S'}\Phi_0'$ and $\text{free}(\Phi') = \emptyset$ and (2.3)
Choose $\mathfrak{I}' = (\mathfrak{A}', \beta')$ st $\mathfrak{I}' \models \Phi'$ and choose, by coincidence lemma, β' st $\beta'(v_n) = c_n^{\mathfrak{A}'}$ for $n \in \mathbb{N}$ ie $\mathfrak{I}'(v_n) = \mathfrak{I}'(c_n)$
Then for $\phi \in \Phi$, substitution lemma $\Rightarrow \mathfrak{I}' \models \phi$ iff $\mathfrak{I}' \models \phi\frac{c_0\dots c_{n(\phi)-1}}{v_0\dots v_{n(\phi)-1}}$
So $\mathfrak{I}' \models \Phi$
So $\text{Sat}\Phi$

5.3. SATISFIABILITY OF CONSISTENT SETS OF FORMULAS (THE GENERAL CASE).

Remark.
- no longer require S ctble
- this section similar to previous section with lem, lem, cor
- will need Zorn's lemma to prove cor

Lemma. *(3.1)*
Assume $\Phi \subset L^S$ with $\text{Con}_S\Phi$
Then there is an $S' \supset S$ and a set $\Psi \subset L^{S'}$ st $\Phi \subset \Psi$ and $\text{Con}_{S'}\Psi$ and Ψ contains witnesses wrt S'
(ie for every formula of the form $\exists x\phi \in L^{S'}$ there is a term $t \in T^{S'}$ st $\Psi \vdash (\exists x\phi \to \phi\frac{t}{x})$

Proof. for lem 2.1, we run out of variables if Φ unctble
overcome this by adding consts to the symbol set which play the role of variables

Lemma. *(3.2)*
Assume $\Psi \subset L^S$ with $\text{Con}_S\Psi$
Then there is a set Θ st $\Psi \subset \Theta \subset L^{S'}$ and Θ is consistent and neg complete wrt S

Proof. see Zorn's lemma (lem 3.5) in a form suited for our purposes

Corollary. *if $\Phi \in L^S$ and $\text{Con}_S\Phi$*
then Φ is satisfiable

5.4. THE COMPLETENESS THM.

Theorem. *(4.1)(Completeness Thm)*
Let $\Phi \subset L^S$ and $\phi \in L^S$
$\Phi \models \phi \Rightarrow \Phi \vdash_S \phi$

Proof. 2.4 for S at most ctble
3.3 for S arbitrary

Claim. *For $\Phi \subset L^S$ and $\phi \in L^S$*
a) $\Phi \models \phi$ iff $\Phi \vdash_S \phi$
b) SatΦ iff Con$_S\Phi$

Proof. a) 4.1, IV.6.2
b) 3.3, IV.7.5

Theorem. *(4.2)(adequacy of the sequent calculus)*
a) $\Phi \models \phi$ iff $\Phi \vdash \phi$
b) SatΦ iff ConΦ

Proof. (see motivation for this thm in footnote on pg 73)
consequence and satisfiability are indep of choice of S (end of III.4)
so derivability and consistency are indep of S
so will can subscript S

Remark. completeness thm first proved by Godel (1928)
this section's method of pf is due to Henkin (1949)

6. THE LOWENHEIM-SKOLEM THM AND THE COMPACTNESS THM

Remark.
- the equivalence of $\vdash$ and $\models$ and of Con and Sat form a bridge between syntax and semantics
  now can transfer properties between $\vdash$ and $\models$ and between Con and Sat
  eg end of previous chapter, dropped subscript S from $\vdash$ since already dropped from Con
- this chapter:
  §2 uses this bridge to get several important results for $\models$ and Sat
  thms of §1 and §2 provide insight to expressive power of first-order languages

6.1. THE LOWENHEIM-SKOLEM THM.

Theorem. *(1.1) (Lowenheim-Skolem thm)*
Let set Φ of formulas be satisfiable and at most ctble
then Φ has a model whose domain is at most ctble

Proof. note: S at most ctble since Φ at most ctble and each $\phi \in \Phi$ has finite number of S-symbols
simple case: Φ S-sentences
then satisfied by $\mathfrak{I}^\Phi$
and underlying set is subsets of T^S which is at most ctble
general case: Φ S-formulas
by pf of (V.2.4), the following two sets are satisfiable over the same domain: Φ and $\Phi' := \{\psi\frac{c_0\dots c_{n-1}}{v_0\dots v_{n-1}} | n \in \mathbb{N}; \psi \in L_n^S \cap \Phi; c_0, ..., c_{n-1} \notin S\}$

Example. can't say anything about finite models...
- sentence $\forall x\forall y x \equiv y$ has only finite models [of size 1?]
- sentence $\forall x\forall y(fx \equiv fy \to x \equiv y) \wedge \neg\forall x\exists y fy \equiv x$ (injective and non-surjective) has only infinite models since there is no function on a finite set which is injective and not surjective

Remark. following thm generalizes above thm for the case of unctble S using concept of "cardinality"

Theorem. *(1.2) ("downward" Lowenheim-Skolem thm)*
if set $\Phi \subset L^S$ is satisfiable
then Φ has a model whose domain is of cardinality not greater than L^S

Remark. rest of section is application of Lowenheim-Skolem to $\mathfrak{R}^<$
[perhaps this belongs at end of chapter in nonstandard models ?]

Claim. *there is no set Φ of $S_{ar}^<$ sentences which characterizes, up to isomorphism, the ordered field $\mathfrak{R}^< = \{\mathbb{R}, +, \cdot, 0, 1, <\}$*
ie can't have exactly $\mathfrak{R}^<$ (and its isomorphism) $\models \Phi$

Proof. assume $\mathfrak{R}^< \models \Phi$
then Φ satisfiable
then by 1.1, there is an at most ctble $\mathfrak{A}$ st $\mathfrak{A} \models \Phi$
but $\mathfrak{A}$ is not isomorphic to $\mathfrak{R}^<$ since $\mathbb{R}$ unctble

Remark. in analysis, $\mathfrak{R}^<$ is characterized (up to isomorphism) by, say, axioms for ordered fields and by the completeness axiom (every nonempty set which is bdd above has a supremum).
axioms for ordered fields can be formulated as $S_{ar}^<$-formulas
so completeness axiom cant be phrased in terms of $S_{ar}^<$-formulas

6.2. THE COMPACTNESS THM.

Remark. recall
a) IV.6.1: $\Phi \vdash \phi$ iff there is a finite $\Phi_0 \subset \Phi$ st $\Phi_0 \vdash \phi$
b) IV.7.4: ConΦ iff for all finite $\Phi_0 \subset \Phi$, ConΦ_0

Theorem. *(2.1)(compactness thm)*
a) $\Phi \models \phi$ iff there is a finite $\Phi_0 \subset \Phi$ st $\Phi_0 \models \phi$
b) SatΦ iff for all finite $\Phi_0 \subset \Phi$, SatΦ_0

Proof. adequacy thm (V.4.2)

Remark.
- the "compactness" thm is reformulation of a thm about a certain topology being compact, see ex 2.5
- Lowenheim-Skolem thm and compactness thm are important to semantics
  also, they are used by Lindstrom (ch XIII) to characterize first-order logic
- next: variants of Lowenheim-Skolem using compactness

Theorem. *(2.2)*
Let set Φ of formulas be satisfiable over arbitrary large finite domains
then Φ is satisfiable over an infinite domain

Proof. Consider $\Psi := \Phi \cup \{\phi_{\geq n} | 2 \leq n\}$.
Any model of Ψ must have an infinite domain since second part.
$\Psi \models \Phi$, so just need to show Ψ is satisfiable.
Ψ is satisfiable since every finite subset satisfiable by model of Φ with large enough domain.
Compactness thm $\Rightarrow \text{Sat}\Psi$.

Theorem. *(2.3) ("upward" Lowenheim-Skolem thm)*
Let set Φ of formulas satisfiable over an infinite domain
Then for every set A, there is a model of Φ which has at least as many elements as A (exists injection of A into model)

Proof. complicated, uses compactness

Claim. *there are arbitrarily large groups, orderings, and fields*

Proof. can be proved using algebraic methods specific to each theory
or proved generally using thm 2.3

Remark.
- previous clm and similar investigations of classes of structures belong to model theory
- next thm generalizes above using "cardinal numbers"

Theorem. *(2.4)(Lowenheim, Skolem, Tarski)*
Let set Φ of formulas which is satisfiable over an infinite domain
Let κ be an infinite cardinal greater than cardinality of Φ
then Φ has a model of cardinality κ

Proof. uses idea pf of 2.3

6.3. ELEMENTARY CLASSES.

Definition. (3.1)
- the class of models of $\Phi \subset L_0^S$ $\mathrm{Mod}^S\Phi := \{\mathfrak{A} : \mathfrak{A}$ is an S-structure and $\mathfrak{A} \models \Phi\}$
  ntn: for singleton $\{\phi\}$, write $\mathrm{Mod}^S\phi$
- Let $\mathfrak{K}$ be a class of S-structures
  $\mathfrak{K}$ is elementary means there is a S-sentence ϕ st $\mathfrak{K} = \mathrm{Mod}^S\phi$
  $\mathfrak{K}$ is Δ-elementary means there is a set Φ of S-sentences st $\mathfrak{K} = \mathrm{Mod}^S\Phi$

Claim. *a) every elementary class is Δ-elementary*
b) every Δ-elementary class is the intersection of elementary classes

Proof. a) by def
b) $\mathrm{Mod}^S\Phi = \cap_{\phi\in\Phi}\mathrm{Mod}^S\phi$

Remark. an algebraic formulation of the expressive power of first-order languages is: which classes of strutures are elementary or Δ-elementary
[see ch XII ?]

Example. (3.2)
elemetary classes:
the class of fields as S_{ar}-structures
the class of ordered fields as $S_{ar}^<$-structures
the class of groups
the class of equivalence strutures
the class of partially ordered fields (cf III.6.4)
the class of directed graphs
pf: $\mathrm{Mod}^S\phi$ where ϕ is a conjunction of finite number of axioms

Definition.
- Let p prime
  field $\mathfrak{F}$ has characteristic p means $\underbrace{1^{\mathfrak{F}} + \cdots + 1^{\mathfrak{F}}}_{p \text{ times}} = 0^{\mathfrak{F}}$
  ie $\mathfrak{F} \models \chi_p$ where $\chi_p := \underbrace{1 + \cdots + 1}_{p \text{ times}} \equiv 0$
- field $\mathfrak{F}$ has characteristic 0 means there is no prime p for which $\mathfrak{F}$ has characteristic p
- ϕ_F :=conjunction of all field axioms

Example.
- for every prime p, the field $\mathbb{Z}/(p)$ ("integers modulo p") has characteristic p
- the field $\mathfrak{R}$ has characteristic 0
- the class of fields of characteristic p can be represented
  $\mathrm{Mod}^{S_{ar}}(\phi_F \wedge \chi_p)$
  note: it is elementary
- the class of fields of characteristic 0 can be represented
  $\mathrm{Mod}^{S_{ar}}(\{\phi_F\} \cup \{\neg\chi_p | p \text{ is prime}\})$
  note: it is Δ-elementary
  following thm and clm says it cant be elementary

Theorem. *(3.3)*
A S_{ar}-sentence which is valid in all fields of characteristic 0 is valid in all fields whose characteristic is sufficiently large

Proof. let ϕ be such an S_{ar}-sentence ie $\{\phi_F\} \cup \{\neg\chi_p | p \text{ is prime}\} \models \phi$
by compactness thm, $\exists n_0$ depending on ϕ st $\{\phi_F\} \cup \{\neg\chi_p | p \text{ is prime}, p < n_0\} \models \phi$

Claim. *the class of fields of characteristic 0 is not elementary*

Proof. Otherwise, there would have to be an S_{ar}-sentence valid precisely in fields of characteristic 0

Example. (application of thm 3.3 to algebra)
Let polynomials $\rho(x), \phi(x)$ have coefs which are relatively prime over all fields of characteristic 0
then coefs are also relatively prime over all fields of sufficiently large characteristic

Proof. write S_{ar}-sentence that says $\rho(x), \sigma(x)$ are relatively prime

Claim. *(3.4)*
the following are not Δ-elementary ie not of form $Mod^S\Phi$
the class of finite S-structures for fixed S
the class of finite groups
the class of finite fields

Proof. otherwise if the classes were of the form $\mathrm{Mod}^S\Phi$
then sentences Φ would have arbitrarily large finite models (eg fields $\mathbb{Z}/(p)$) but no infinite model
contradicts 2.2

Claim. *the corresponding classes of infinite S-structures are Δ-elementary*
similarly for infinite groups and infinite fields

Proof. ex 3.7
[since need non-finite number of axioms?]

Claim. *(3.5)*
the class of torsion groups is not Δ-elementary

Proof. need cyclic groups, see book

Claim. *(3.6)*
the class of connected graphs (graph (G, R^G) st $\forall a, b \in G$, $a \neq b$, there are $n \geq 2$ and $a_1, \ldots, a_n \in G$ with ($a_1 = a, a_n = b$, and $R^G a_i a_{i+1}$ for $i = 1, \ldots, n-1$) ie distinct elements have a path) is not Δ-elementary

Proof. by contradiction; uses n-gons

6.4. ELEMENTARILY EQUIVALENT STRUCTURES.

Definition. (4.1)
- S-structures $\mathfrak{A}, \mathfrak{B}$ are elementarily equivalent ("$\mathfrak{A} \equiv B$") means for every S-sentence ϕ, $\mathfrak{A} \models \phi$ iff $\mathfrak{B} \models \phi$
- the (first-order) theory of S-structure $\mathfrak{A}$ is $\mathrm{Th}(\mathfrak{A}) := \{\phi \in L_0^S | \mathfrak{A} \models \phi\}$
- $\mathfrak{A}$ is characterized up to isomorphism means there is a Φ st $\mathrm{Mod}^S\Phi = \{\mathfrak{B} | \mathfrak{A} \cong \mathfrak{B}\}$

Lemma. *(4.2)*
$\mathfrak{B} \equiv \mathfrak{A}$ *iff* $\mathfrak{B} \models Th(\mathfrak{A})$

Proof. ($\Rightarrow$) $\mathfrak{B} \equiv \mathfrak{A}$ and $\mathfrak{A} \models \mathrm{Th}(\mathfrak{A}) \Rightarrow \mathfrak{B} \models \mathrm{Th}(\mathfrak{A})$
($\Leftarrow$) $\mathfrak{B} \models \mathrm{Th}(\mathfrak{A})$ then given S-sentence ϕ
case $\mathfrak{A} \models \phi$: then $\phi \in \mathrm{Th}(\mathfrak{A})$ then $\mathfrak{B} \models \phi$
case not $\mathfrak{A} \models \phi$: then $\neg\phi \in \mathrm{Th}(\mathfrak{A})$ so $\mathfrak{B} \models \neg\phi$ so not $\mathfrak{B} \models \phi$

Remark. Consider classes $\{\mathfrak{B} | \mathfrak{B} \cong \mathfrak{A}\}$ and $\{\mathfrak{B} | \mathfrak{B} \equiv \mathfrak{A}\}$ ie the class of structures isomorphic to $\mathfrak{A}$ and the class of structures elemetarily equivalent to $\mathfrak{A}$.
Isomorphism lemma $\Rightarrow$ isomorphic structures are (a subclass of) elementarily equivalent structures
next thm and cor say it is a proper subclass

Theorem. *(4.3)*
a) if $\mathfrak{A}$ is infinite then the class $\{\mathfrak{B} | \mathfrak{B} \cong \mathfrak{A}\}$ is not Δ-elementary
ie no infinte structure can be characterized up to isomorphism in a first-order language
b) for every sturcture $\mathfrak{A}$, the class $\{\mathfrak{B} | \mathfrak{B} \equiv \mathfrak{A}\}$ is Δ-elementary
moreover, $\{\mathfrak{B} | \mathfrak{B} \equiv \mathfrak{A}\}$ is the smallest Δ-elementary class which contains $\mathfrak{A}$

Proof.
a) Towards contradiction, assume $\mathfrak{A}$ infinite and let S-sentences Φ st $\mathrm{Mod}^S\Phi = \{\mathfrak{B} | \mathfrak{B} \cong \mathfrak{A}\}$
Φ has an infinite model
so 2.3 $\Rightarrow$ Φ has a model $\mathfrak{B}$ with at least as many elements as the power set of A
so $\mathfrak{B}$ is not isomorphic to $\mathfrak{A}$
contradiction
b) 4.2 $\Rightarrow \{\mathfrak{B} | \mathfrak{B} \equiv \mathfrak{A}\} = \mathrm{Mod}^S\mathrm{Th}(\mathfrak{A})$
if $\mathrm{Mod}^S\Phi$ is another Δ-elementary class containing $\mathfrak{A}$ then $\mathfrak{A} \models \Phi$
then $\mathfrak{B} \models \Phi$ for every $\mathfrak{B}$ st $\mathfrak{B} \equiv \mathfrak{A}$
so $\{\mathfrak{B} | \mathfrak{B} \equiv \mathfrak{A}\} \subset \mathrm{Mod}^S\Phi$

Corollary. *(4.4)*
for infinite $\mathfrak{A}$, $\{\mathfrak{B} | \mathfrak{B} \cong \mathfrak{A}\} \subsetneq \{\mathfrak{B} | \mathfrak{B} \equiv \mathfrak{A}\}$
ie for each infinite structure there exists an elementarily equivalent, non-isomorphic structure

Remark.
- 4.3b shows that a Δ-equivalent class contains, together with any given structure, all elementarily equivalent ones
- can use this fact to show that a class $\mathfrak{K}$ is not Δ-elementary by specifying two elementarily equivalent structures, one of which belongs to $\mathfrak{K}$ and the other does not
- this method is illustrated for archimidean fields

Definition. ordered field $\mathfrak{F}$ is archimedean means for every $a \in F$ there is $n \in \mathbb{N}$ st $a <^F \underbrace{1^F + \cdots + 1^F}_{n \text{ times}}$
eg ordered field of rationals and ordered field $\mathfrak{R}^<$ of reals

Theorem. *(4.5)*
the class of archimedean fields is not Δ-elementary

Proof. will show there is an ordered field elementarily equivalent to $\mathfrak{R}^<$ which is not archimedean
Let $\Psi := Th(\mathfrak{R}^<) \cup \{0 < x.1 < x.2 < x, ...\}$
where $0.1, 2, ...$ stand for S_{ar}-terms $0, 1, 1+1, ...$
compactness thm $\Rightarrow$ SatΨ (say by $(\mathfrak{A}, \beta)$) since every finite subset satisfiable by $(\mathfrak{R}^<, \beta)$ where $\beta(x)$ is sufficiently large.
Note $\mathfrak{A} \equiv \mathfrak{R}^<$ since $\mathfrak{A} \models Th(\mathfrak{R}^<)$.
But $\mathfrak{A}$ not archimedean since $\beta(x) \in A$ is does not satisfy archimedean property (it is "infinitely large")

Remark.
- compactness thm was used in proof of 2.2, 2.3, 3.5, 4.5
  in each case, needed to find a structure with certain properties which can be expressed in first-order logic by means of a suitable set Ψ of formulas, and compactness was employed to prove satisfiability of Ψ
- eg in pf of 4.5, Ψ contains, in addition to $\mathrm{Th}(\mathfrak{R}^<)$, formulas which guarantee an element violates the archimidean ordering property
  and since there exists ordered fields with arbitrarily large finite elements so compactness implies there exist an ordered field with an "infinitely large" element
- Skolem's thm below is further applications to this method of pf

Definition. nonstandard model of $\mathfrak{A}$ is a structure which is elementarily equivalent, but not isomorphic to $\mathfrak{A}$

Remark.
- 4.4 $\Rightarrow$ $\mathfrak{N}$ cannot be characterized up to isomorphism by means of first-order formulas (cf 4.4)
- aside: axioms Π (ex III.7.5) (with second-order induction axiom) characterizes $\mathfrak{N}$ up to isomorphism
- 2.3 $\Rightarrow$ there is an unctble nonstandard model of arithmetic. Next thm shows there is a ctble nonstandard model of arithmentic

Theorem. *(4.6) (Skolem's thm)*
there is a countable nonstandard model of arithmetic

Proof. Let $\Psi := Th(\mathfrak{N}) \cup \{\neg x \equiv 0, \neg x \equiv 2, \neg x \equiv 3, ...\}$
compactness thm $\Rightarrow$ Ψ satisfiable by some $(\mathfrak{A}, \beta)$ since every finite subset satisfiable.
Lowenheim-Skolem $\Rightarrow$ $\mathfrak{A}$ at most ctble, so ctble since rhs
$\mathfrak{A} \equiv \mathfrak{N}$ since for $m \neq n$, $\neg m \equiv n \in Th(\mathfrak{A})$
$\mathfrak{A} \ncong \mathfrak{N}$ since bijection $\pi : A \to \mathbb{N}$ and $\pi(\beta(x)) \notin \mathbb{N}$

Theorem. *(4.7)*
there is a ctble nonstandard model of $Th(\mathfrak{N}^<)$

Proof. exactly like 4.6; but with set $\mathrm{Th}(\mathfrak{N}^<) \cup \{\neg x \equiv 0, \neg x \equiv 1, \neg x \equiv 2, ...\}$

Remark.
- what does a nonstandard model $\mathfrak{A}$ of $\mathrm{Th}(\mathfrak{N}^<)$ look like?
  in $\mathfrak{N}^<$ the sentences $\forall x(0 \equiv x \vee 0 < x)$
  $0 < 1 \wedge \forall x(0 < x \to (1 \equiv x \vee 1 < x))$
  $1 < 2 \wedge \forall x(1 < x \to (2 \equiv x \vee 2 < x)), \ldots$ hold.
  they say that 0 is the smallest element, 1 is next smallest, 2 is next smallest, ...
  $\mathfrak{N}^<$ and $\mathfrak{A}$ have "initial segment" which looks like a number line $0^A, 1^A, 2^A, \ldots$
  In additio, $\mathfrak{A}$ holds further elements on number line
  see book for more and images
- examples in this and previous section illustrate important classes of structures which cannot be axiomatized in first-order logic
  but this weakness in expressive power leads to pleasant results:
  -establishing that the class of archimedian fields is not axiomatizable yields a proof of the existence of non-archimedian ordered fields
  -the class of fields of characteristic 0 cannot be axiomatized by a single S_{ar}-sentence is complemented by the interesting result 3.3
- using similar methods, can obtain structures elementarily equivalent to ordered field $\mathfrak{R}^<$ which contain, in addition to reals, infinitely large elements and infinitely small elements (called infinitesimals).
  such structures can be used to develop "nonstandard analysis" which avoids the ϵ-δ-technique

7. THE SCOPE OF FIRST-ORDER LOGIC

Remark.
- investigations of logical reasoning used in Math led to formalization of propositions and proof in first-order language
  then completeness thm showed that mathematical proof coincides with formal proof, provided the propositions and axioms admit a first-order formulation
- §1: we used math proofs before defining formal proof.
  are we caught in a viscous cycle? if not, how can we justify the rules of sequent calculus $\mathfrak{G}$?
  Answer: formal proofs can be introduced without math proofs
- §2: does limited expressive power of first-order languages limit the scope of our investigation?
  Answer: first-order logic is sufficient for present-day math
  ie a finite set S of conrete symbols suffices to represent the statements and arguments arising in Math

7.1. THE NOTION OF FORMAL PROOF.

Remark.
- will consider concrete symbols and strings of these symbols (terms, formulas, sequents) and not abstract math entities eg not formulas in $S = \{c_r | r \in \mathbb{R}\}$
- formal pf is syntactic operations on symbol strings governed by calculi of terms, formulas, and sequents
  formal pf is sequence of sequents each obtained by applying a sequent rule to preceding sequents
- analogy: rules of chess allow certain operations on pieces
  rules are simple, can be checked by anyone
  need not know the meaning behind the moves
  skilled players make better moves

Claim. *can avoid math proof when developing formal pfs*

Proof. incomplete pf:
unique decomposition of sequent to get antecedent can be replaced by keeping record of how symbols strings were built
see book for using ($\vee$A), ($\equiv$), ($\exists$A)

Remark.
- Math is also creative development of proof ideas, introduction of adequate concepts, setting up suitable systems of axioms, and finding new interesting conjectures
- formal character of formal proofs allow computers to systematically produce proofs and to check correctness
  see limitations in ch X, XI
- we have merely imitated methods of inference, not justified them

Definition.
- classical mathematicians require every proposition to be either true or false (tertium non datur)
  math objects exist without our knowledge of them
- intuitionalist mathematicians require constructive proofs of math propostions
  math objects exist only as ideas
  [wiki: Intuitionism]

Example. Goldbach conjecture A
A: every even ≥ 4 is the sum of two primes
not A: not every even ≥ 4 is the sum of two primes
classical point of view: (A or not A) is true
intuitionalist point of view: (A or not A) cannot be asserted since neither proposition A nor not A have hitherto been proved

Remark. We will use classical point of view

7.2. MATH WITHIN THE FRAMEWORK OF FIRST-ORDER LOGIC.

Example. recall (III.7.3)
arithmetic structure $\mathfrak{N}_\sigma = (\mathbb{N}, \sigma, 0)$ cannot be characterized up to isomorphism by first-order sentences, but (Dedekind's thm, III.7.4) can be by peano axioms which are second-order sentences

Definition.
- peano axioms
  (P1) $\forall x \neg \sigma x \equiv 0$
  (P2) $\forall x \forall y(\sigma x \equiv \sigma y \to x \equiv y)$
  (P3) $\forall X((X0 \wedge \forall x(Xx \to X\sigma x)) \to \forall y Xy)$
- peano structure is any structure satisfying (P1),(P2),(P3)

Theorem. *(2.1)(reformulate Dedekind's thm)*
Any two Peano structures are isomorphic

Remark.
- even though Peano structures cant be characterized in first-order language, can formulate (2.1) and its pf (which involves (P3)) in first-order language
  will show how
- need domain to include all peano structures, isomorphisms between each pair of structures, all elements of these peano structures, and all subsets of these peano structures
- let domain be the mathematical universe (all objects which are treated in mathematics; totality of mathematical objects)
  note: contains natural numbers, points, sets, functions, structures, topological spaces, and also the set $\{a_1, a_2\}$ of each pairs of objects a_1, a_2, the union $M_1 \cup M_2$ of any two sets M_1, M_2, and the inverse f^{-1} of any injective function f
- Let symbol set S suitable for the universe
- Let set $\Phi_0 \subset L_0^S$ of all properties of the universe which mathematicians use, (this section will present parts of Φ_0, next section will present complete system Φ_0)
- will formalize (2.1) as a proposition in L^S about the universe

Definition.
- urelements are the "simple" objects (eg numbers, points,...) of the universe
- sets are the "complex" objects (eg functions, ordered pairs, ...) of the universe
  contain elements which are urelements and sets

Remark. so we are dealing with sets
so Φ_0 is a system of axioms for set theory
ie the set-theoretic assumptions about the universe upon which the mathematician relies

Definition.
- $S := \{U, M, \in\}$
  U is unary relation symbol meaning "... is a urelement"
  M is unary relation symbol meaning "... is a set"
  $\in$ is binary relation "... is an element of ..."
- Φ_0 (see next section for the rest):
  (A1) $\forall x(Ux \vee Mx)$
  "every object of the universe is an urelement or a set"
  (A2) $\forall x \neg(Ux \wedge Mx)$
  "no object is both an urelement and a set"
  (A3) $\forall x \forall y((Mx \wedge My \wedge \forall z(z \in x \leftrightarrow z \in y)) \to x \equiv y)$
  "two sets which contain the same elements are equal"
  (A4) $\forall x \forall y \exists z(Mz \wedge \forall u(u \in z \leftrightarrow (u \equiv x \vee u \equiv y)))$
  "for every two objects x and y, the pair set $\{x, y\}$ exists"
- ordered pair (x, y) is $\{\{x, x\}, \{x, y\}\}$
  yielded by repeated application of (A4)
- ordered triples are $(x, y, z) := ((x, y), z)$

Claim.
- *z which exists by (A4) is unique by (A3)*
- *$(x, y) = (x', y')$ iff $x = x'$ and $y = y'$*
  pf: use (A1)-(A4)

Definition. abbreviations:
($\subset$) $x \subset y$ for $Mx \wedge My \wedge \forall z(z \in x \to z \in y)$
"x is a subset of y"
(could have added binary relation symbol $\subset$ to S and added axiom to Φ_0 $\forall x \forall y(x \in y \leftrightarrow (Mx \wedge My \wedge \forall z(z \in x \to z \in y)))$)
(OP) $OPzxy$ for $Mz \wedge \forall u(u \in z \leftrightarrow (Mu \wedge (\forall v(v \in u \leftrightarrow v \equiv x) \vee \forall v(v \in u \leftrightarrow (v \equiv x \vee v \equiv y)))))$
"z is the ordered pair of x and y"
(OT) $OTuxyz$ for $Mu \wedge \exists v(OPuvz \wedge OPvxy)$
"u is the ordered triple (x, y, z)"
(E) $Euxy$ for $Mu \wedge \exists z(z \in u \wedge OPzxy)$
"the ordered pair (x, y) is an element of u"
(F) Fu for $Mu \wedge \forall z(z \in u \to \exists x \exists y OPzxy) \wedge \forall x \forall y \forall y'((Euxy \wedge Euxy') \to y \equiv y')$
"u is a function, that is, a set of ordered pairs (x, y), where y is the value of u at x"
ie $f : A \to B$ is considered as set $\{(x, f(x)) | x \in A\}$, which is also referred to as the graph of f
(D) Duv for $Fu \wedge Mv \wedge \forall x(x \in v \leftrightarrow \exists y Euxy)$
"v is the domain of the function u"

(R) Ruv for $Fu \wedge Mv \wedge \forall y(y \in v \leftrightarrow \exists x Euxy)$
"v is the range of the function u"

Remark. we consder a $\{\sigma, 0\}$-structure as an ordered triple (x, y, z) consisting of set x, function $y : x \to x$, and an element $z \in x$
this is contrary to convention in III.1.1

Definition.
(PS) PSu for $\exists x \exists y \exists z(OTuxyz \wedge Mx \wedge z \in x \wedge Fy \wedge Dyx \wedge \exists v(Ryv \wedge v \subset x) \wedge (1) \wedge (2) \wedge (3))$
where peano axioms are reformulated
(1) $\forall w(w \in x \to \neg Eywz)$
(2) $\forall w \forall w' \forall v((Eywv \wedge Eyw'v) \to w \equiv w')$
(3) $\forall x'((x' \subset x \wedge z \in x' \wedge \forall w \forall v((w \in x' \wedge Eywv) \to v \in x')) \to x' \equiv x)$
"u is a Peano structure"
(I) $Iwuu'$ for *long, see book*
"w is an isomorphism of Peano structure u onto Peano structure u'"

Theorem. *(2.2) (reformulation of (2.1) in L^S)* $\Phi_0 \vdash \forall u \forall v(PSu \wedge PSv \to \exists w Iwuv)$
ie for every two peano structures $\mathfrak{A}, \mathfrak{B}$ in the universe, there is another object, an isomorphism between $\mathfrak{A}$ and $\mathfrak{B}$

Proof. reformulate pf of Dedekind's thm (III.7) to L^S

Remark.
- reformulation of Dedekind's thm to L^S was possible since set theory treats all objects in the universe as first-order ones
- more generally, experience suggests that (i) all math propositions can be formulated in L^S (or variants of it) and (ii) all mathematically provable propositions are derivable from Φ_0
- thus it may be possible to imitate all mathematical reasoning in L^S using the sequent calculus
  ie first-order logic may be sufficient for all of math

Definition.
- background set theory is Φ_0 as the properties of the math universe; the background for all math considerations
- object set theory is Φ_0 in the context of studying Φ_0 itself

Remark.
- be careful when distinguishing object set theory and background set theory
  eg a model $\mathfrak{A} = \{A, U^A, M^A, \in^A\}$ of Φ_0 and underlying set A are objects of the universe thus in the domain of background set thoery
  so A is distinct from the universe in background set theory.
  All set-theoretic statements (which are derivable from Φ_0) hold in $\mathfrak{A}$
  But $a \in^A b$ holding in object set thoery does not mean that $a \in b$ holds in background set theory
- section 4: confusion between background and object set theory result in paradoxes
  eg Skolem's paradox: there are unctbly many sets (eg unctbly many subsets of $\mathbb{N}$)
  this fact can be formalized by sentence ϕ derivable from Φ_0.
  But Lowenheim-Skolem thm $\Rightarrow$ there is a ctble model of $\mathfrak{A}$ of Φ_0 and hence of ϕ
  thus a ctble model $\mathfrak{A}$ satisfies a sentence which says that there are unctbly many sets in $\mathfrak{A}$

7.3. THE ZARMELO-FRAENKEL AXIOMS FOR SET THEORY.

Remark.
- this section will present full system of axioms for set theory
- abandon the use of urelements since can replace urelements by suitable sets eg elements of $\mathbb{N}$ later this section
- so can abandon symbols U, M
- so formulate axioms in $L^{\{\in\}}$, where the variables are intended to range over the sets of the universe
- next will formulate ZFC axioms (Zarmelo-Fraenkel-Skolem including axiom of choice)

Definition. ZFC axioms
(EXT) (the axiom of extensionality)
$\forall x \forall y(\forall z(z \in x \leftrightarrow z \in y) \to x \equiv y)$
"two sets which contain the same elements are equal"
(SEP) (seperation axioms)
for each $\phi(z, x_1, ..., x_n)$ (ntn: $z, x_1, ..., x_n$ occur free in ϕ) and arbitrary variables x, y distinct and distinct from z, x_i
$\forall x_1 ... \forall x_n \forall x \exists y \forall z(z \in y \leftrightarrow (z \in x \wedge \phi(z, x_1, ..., x_n)))$
"given a set x and a property P which can be formulated by an $\{\in\}$-formula ϕ, the set $\{z \in x | z$ has property P$\}$" exists
($PAIR$) (the pair set axiom)
$\forall x \forall y \exists z \forall w(w \in z \leftrightarrow (w \equiv x \vee w \equiv y))$
"given two sets x, y, the pair set $\{x, y\}$ exists"
(SUM) (the sum set axiom)
$\forall x \exists y \forall z(z \in y \leftrightarrow \exists w(w \in x \wedge z \in w))$
"given a set x, the union of all sets in x exists"
(POW) (the power set axiom)
$\forall x \exists y \forall z(z \in y \leftrightarrow \forall w(w \in z \to w \in x))$
"given a set x, the power set of x exists"

Remark. ntn, see book for formulas
($\emptyset$) (constant for the empty set)
$\forall y(\emptyset \equiv y \leftrightarrow \forall z \neg z \in y)$
($\subset$) (binary relation symbol for the subset relation)
($\{,\}$) (binary function symbol for pairing)
ntn: for term $\{y, y\}$ write $\{y\}$
($\cup$) (binary function symbol for the union)
($\cap$) (binary function symbol for the intersection)
(P) (unary function symbol for the power set operation)

Definition. rest of ZFC axioms, see book for formulas
(INF) (the axiom of infinity)
"there exists and infinite set, namely a set containing $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots$"
(REP) (replacement axioms)
"if for parameters $x_1, \ldots, x_n$ the formula $\phi(x, y, x_1, \ldots, x_n)$ defines a map $x \mapsto y$, then the range of a set is again a set"
(AC) (the axiom of choice)
"given a set x of nonempty pairwise disjoint sets, there exists a set which contains exactly one element of each set in x."

Remark. can now introduce notion of ordered pair, function, etc like previous section.
can now, by examples, give evidence that (1) all math propositions can be formalized in $L^{\{\in\}}$ and that (2) provable propositions correspond to sentences derivable in ZFC

Example. can replace natural numbers by suitable sets
pf: represent the natural numbers as sets $\tilde{0} := \emptyset$, $\tilde{1} := \{\emptyset\} = \{\tilde{0}\}$, $\tilde{2} := \{\emptyset, \{\emptyset\}\} = \{\tilde{0}, \tilde{1}\}$, ..., $\tilde{n} := \{\tilde{0}, \tilde{1}, ..., n\tilde{-}1\}$
note: these sets are inductive (if contains x then contains $x \cup \{x\}$), and the smallest inductive set represents $\mathbb{N}$

Claim. *"there is a smallest inductive set" is derivable in ZFC*

Proof. by INF, there exists an inductive set, say x.
SEP gives set $\omega := \{z | z \in x$ and for all inductive $y, z \in y\}$
this set is the smallest inductive set ie ω is inductive and for every inductive y, $\omega \subset y$

Remark.
- $(\omega, v, 0)$ is a Peano structure, where $v = \{(x, x \cup \{x\}) | x \in w\}$ is successor function
  this Peano structure can play the role of $\mathfrak{N}_\sigma$
- rest of section about something ZFC cant prove or disprove
  [ie ZFC is incomplete]

Definition.
- sets x, y are of same cardinality ("$x \sim y$") means there is a bijection x to y
- finite set have same cardinality as an element of ω
  ctble set has the same cardinality as ω
  the continuum of $\mathbb{R}$ is unctble
- (CH) Continuum Hypothesis
  $\forall x((x \subset \mathbb{R} \wedge \neg \mathrm{Fin} x) \to (\mathrm{Count} x \vee x \sim \mathbb{R}))$
  "every infinite subset of $\mathbb{R}$ is either ctble or of same cardinality as $\mathbb{R}$"
  first stated by G. Cantor in late 1800s

Theorem. *(3.1) If ZFC is consistent then not $ZFC \vdash \neg CH$*

Proof. Godel, 1938

Theorem. *(3.2) If ZFC is consistent then not $ZFC \vdash CH$*

Proof. Cohen, 1963

Remark.
- if ZFC consistent, then neither CH nor $\neg$CH is derivable from it.
- so our concept of set theory, which ZFC embodies, is too vague to decide CH
- in X.7, will show that cant give "explicitly" an axiom system Ψ for set theory which decides every set-theoretic statement (in the sense that for every $\{\in\}$-sentence ψ, either $\Psi \vdash \psi$ or $\Psi \vdash \neg\psi$)

7.4. SET THEORY AS A BASIS FOR MATH.

Remark. this section:
4.1: how the question of consistency of math can be made precise by use of suitable first-order axioms sufficient for math
4.2: misunderstandings arising from confusion of object set theory with background set theory
4.3: how first-order logic, like every other math theory, can be based on set theory

Remark. (4.1)
- experience shows that math statements can be formalized in $L^\in$ and provable statements derived from ZFC.
  assume this is always the case
- Hilbert wanted to show ZFC is consistent ie there is no ϕ st ZFC$\vdash \phi$ and ZFC$\vdash \neg\phi$, which would suggest "the generally accepted methods of math taken as a whole do not lead to a contradiction"
  ie wanted no derivation of sequent $\phi_1 ... \phi_n(\phi \wedge \neg\phi)$ where $\phi_1, ..., \phi_n$ are ZFC axioms
- Godel's second incompleteness thm (X.7) shows that such a consistency proof for ZFC is not possible, even using all of the auxiliary means of background set theory
- in particular, cant prove existence of a model of ZFC, since Sat implies Con
- but ZFC has been used for decades without an inconsisitency found, so we assume ZFC to be consistent

Remark. (4.2)
two examples, see book for details
- Skolem's paradox
  todo
- consider set of sentences $\Psi :=$ZFC$\cup\{c_r \in w | r \in \mathbb{R} \cup \{\neg c_r \equiv c_s | r, s \in \mathbb{R}, r \neq s\}\}$
  todo

Remark. (4.3)

- will provide a set-theoretic development of first-order logic
- note: we already converted functions and Peano structures to sets
- consider symbol set $S = \{P^1, P^2, \dots\}$ with n-ary P^n
- first need a set-theoretic substitute for S-formulas
- substitute for variables with elements $\tilde{0}, \tilde{1}, \dots$ of ω
  replace symbols $\neg, \vee, \exists, \equiv$ with ordered pairs $\tilde{\neg} := (\tilde{0}, \tilde{0})$, $\tilde{\vee} := (\tilde{0}, \tilde{1})$, $\tilde{\exists} := (\tilde{0}, \tilde{2})$, $\tilde{\equiv} := (\tilde{0}, \tilde{3})$
  (similarly, could, for example, let ordered pairs $(\tilde{2}, x)$ with $x \in \omega$ stand for functions)
  to represent symbol sets with unctbly many elements, use an appropriate set of larger cardinality instead of ω
- now formula $v_n \equiv v_m$ corresponds to triple $x, \tilde{\equiv}, y)$ with $x, y \in \omega$
  these triples are elements of the set $At^{\equiv} := \omega \times \{\equiv\} \times \omega$
  formula $P^n v_{m_0} \dots v_{m_{n-1}}$ correspond to ordered pair $(\tilde{P}^x, z)$ where $x \in \omega$ and z is function from x into ω
  (eg $P^3 v_1 v_4 v_5$ corresponds to $(\tilde{P}^{\tilde{3}}, z)$ with $z = \{(\tilde{0}, \tilde{1}), (\tilde{1}, \tilde{4}), (\tilde{2}, \tilde{5})\}$)
  The set of atomic "relational" formulas is $At^R := \{(\tilde{P}^x, z) | x \in \omega \text{ and } z : x \to \omega)\}$
  define the set of all S-formulas to be the smallest set A st
  (1) $At^{\equiv} \cup At^R \subset A$
  (2) if $y \in A$ then $(\tilde{\neg}, y) \in A$
  (3) if $y, z \in A$ then $(y, \tilde{\vee}, z \in A)$
  (4) if $x \in \omega$ and $y \in A$ then $(\tilde{\exists}, x, y) \in A$
- now can give set-theoretic description of syntax of sequent, derivation
  can give set-theoretic description of semantics of structures and consequence
  can can obtain a set-theoretic formulation of completeness thm as $\{\in\}$-sentence, and derive it in ZFC
- benefits of set-theoretic interpretation:
  (1) our mathematical development of first-order logic can be founded upon the axiomatic basis ZFC
  (2) can deal with unctble symbol sets in a precise manner
  can define other languages eg those with infinitely long "formulas" of the form $\phi_0 \vee \phi_1 \vee \phi_2 \vee \dots$ (ch IX)
  (3) completeness thm required a proof, leading to visious cycle in VII.1
  in the set-theoretic framework, we can see that the assumptions needed for proof of completeness thm can be weaker than ZFC

8. SYNCTACTIC INTERPRETATIONS AND NORMAL FORMS

Remark. this chapter
- will show to which extent the choice of a symbol set is arbitrary
  eg S_{grp} and S_{gr} have same expressive power for group theory
- will see that syntactic interpretation is important
- §4: for different syntactic properties, can find logically equiv formula which has this property
  ie can put into syntactically simpler form

8.1. TERM-REDUCED FORMULAS AND RELATIONAL SYMBOL SETS.

Definition.
- nested function symbol eg Rgx has nested gx
- term-reduced S-formula means its atomic subformulas have the form $Rx_1 \dots x_n$, $x \equiv y$, $fx_1 \dots x_n \equiv x$, or $c \equiv x$

Example. $\{f, g\}$-formula $\phi := \forall x f g x \equiv y$ has nested gx
term-reduced formula is $\forall x \exists u (gx \equiv u \wedge fu \equiv y)$
note: these formulas are logically equiv

Theorem. *for every S-formula ψ there is a logically equiv term-reduced S-formula ψ^* with free(ψ) =free(ψ^*)*

Proof. define t^* and ϕ^* by induction on terms and formulas

Remark. sometimes convenient to deal with symbol set of only relations (see ch XII)

Definition.
- relational symbol set contains only relation symbols
- S^r by taking arbitrary S
  replace n-ary function symbol $f \in S$ with $(n+1)$-ary relation symbol representing its graph
  replace const symbol $c \in S$ with unary relation symbol C
  note: S^r is relational
- S^r-structure $\mathfrak{A}^r$ from S-structure $\mathfrak{A}$
  1) $A^r := A$
  2) for $P \in S$, $P^{\mathfrak{A}^r} := P^{\mathfrak{A}}$
  3) for n-ary $f \in S$, $F^{\mathfrak{A}^r} :=$ the graph of $f^{\mathfrak{A}}$
  4) for $c \in S$, $C^{\mathfrak{A}^r} :=$ the graph of $c^{\mathfrak{A}}$ ie $C^{\mathfrak{A}^r} a$ iff $c^{\mathfrak{A}} = a$

Theorem. *(1.3)*
a) for every $\psi \in L^S$ there is $\psi^r \in L^{S^r}$ st for all S-interpretations $(\mathfrak{A}, \beta)$, $(\mathfrak{A}, \beta) \models \psi$ iff $(\mathfrak{A}^r, \beta) \models \psi^r$
b) for every $\psi \in L^{S^r}$, there is $\psi^{-r} \in L^S$ st for all S-interpretations $(\mathfrak{A}, \beta)$, $(\mathfrak{A}, \beta) \models \psi^{-r}$ iff $(\mathfrak{A}^r, \beta) \models \psi$

Proof. a) inductively define ψ^r for term reduced ψ
b) similarly, but must define $[ft_1 \dots t_n t]^{-r}$ and $[Ct]^{-r}$

Corollary. *(1.4)*
for two S-structures $\mathfrak{A}, \mathfrak{B}$,
$\mathfrak{A} \equiv \mathfrak{B}$ iff $\mathfrak{A}^r \equiv \mathfrak{B}^r$

8.2. SYNTACTIC INTERPRETATIONS.

Remark. this section: A-D are motivating examples, then E is defs and thms about syntactic interpretations

(A) AXIOM SYSTEMS FOR GROUPS

Remark.
- recall Φ_{gr} in $L_0^{S_{gr}}$ with $S_{gr} = \{\circ, e\}$
  recall Φ_{grp} in $L_0^{S_{grp}}$ with $S_{grp} = \{\circ, ^{-1}, e\}$
- define Φ_g in $L_0^{S_g}$ with $S_g = \{\circ\}$ as
  $\Phi_g := \{\forall x \forall y \forall z (x \circ y) \circ z \equiv x \circ (y \circ z), \exists z (\forall x x \circ z \equiv x \wedge \forall x \exists y x \circ y \equiv z)\}$
- all three axiom systems are equivalent - the same statements are expressible and the same statements are provable

Example. S_{grp} sentence $\forall x x \circ x^{-1} \equiv e$ corresponds to S_g-sentence $\exists z (\forall x x \circ z \equiv x \wedge \forall x \exists y x \circ y \equiv z)$

(B) AXIOM SYSTEMS FOR ORDERINGS

Remark.
- recall Φ_{ord} in L_0^S with $S = \{<\}$ (III.6.4)
- define $S' = \{<, \leq\}$ and $\Phi'_{ord} := \Phi_{ord} \cup \{\forall x \forall y (x \leq y \leftrightarrow (x < y \vee x \equiv y))\}$
- can always replace $\leq$ with its def which is the second part of Φ'_{ord}
  so can associate each S'-formula ϕ with S-formula $\phi^<$ st
  $\Phi'_{ord} \models \phi$ iff $\Phi_{ord} \models \phi^<$
- in this sense, L^S and $L^{S'}$ have the same expressive power for the class of orderings

(C) RINGS

Remark.
- define the axioms for "rings with 1"
  $\Phi_{rg} := \Phi_{fd} \setminus \{\forall x (\neg x \equiv 0 \to \exists y x \cdot y \equiv 1), \forall x \forall y x \cdot y \equiv y \cdot x\}$
  ie exclude existence of multiplicative inverse and multiplicative commutativity
- every field (as an S_{ar}-structure) is a ring
- examples
  -the ring of integers uses $\mathbb{Z}$, usual operations
  -for $n \geq 1$ the $n \times n$ mxs of $\mathbb{R}$ (with usual operations) forms ring $\mathfrak{M}(n)$
- unit in ring $\mathfrak{A}$ is all $a \in A$ st there is $b \in A$ st $a \cdot^{\mathfrak{A}} b = b \cdot^{\mathfrak{A}} a = 1$
  formally, let $\epsilon := \exists y (x \cdot y \equiv 1 \wedge y \cdot x \equiv 1)$ then the set of units in $\mathfrak{A}$ is $E(\mathfrak{A}) := \{a \in A | \mathfrak{A} \models \epsilon[a]\}$
- eg ring of integers has units -1,1
  eg $\mathfrak{M}(n)$, the units are invertible mxs
- note $1^{\mathfrak{A}} \in E(\mathfrak{A})$ and $E(\mathfrak{A})$ is closed under multiplication
- so $E(\mathfrak{A})$ with $1^{\mathfrak{A}}$ and multiplication forms the group (as S_{gr}-structures) of units of $\mathfrak{A}$
- $\mathfrak{A}$ can talk about $E(\mathfrak{A})$ in the sense that for every $\phi \in L_0^{S_{gr}}$ there exists $\phi' \in L_0^{S_{ar}}$ st
  $E(\mathfrak{A}) \models \phi$ iff $\mathfrak{A} \models \phi'$
- eg $\phi := \forall x \forall y x \circ y \equiv y \circ x$ ie commutative axiom then S_{ar}-sentence $\phi' = \forall x \forall y ((\epsilon \wedge \epsilon \frac{y}{x}) \to x \cdot y \equiv y \cdot x)$

(D) RELATIVIZATIONS

Definition. relativization of a formula is another formula which restricts values to specific sets

Example.
- in translating the commutative law to the language of rings, had to restrict quantifiers to the set of units
- (III.7.2) for vector space as a one-sorted structure, need to reletivize field axioms to scalars and group axioms to vectors
  eg field axiom $\forall x (\neg x \equiv 0 \to \exists y x \cdot y \equiv 1)$ is reformualted to $\forall x (\underline{F}x \to (\neg x \equiv 0 \to \exists y (\underline{F}y \wedge x \cdot y \equiv 1)))$
  eg field formula $\phi := \forall x (x \equiv 0 \vee x \equiv 1)$ reletivized to $\underline{F}$ becomes $\phi^{\underline{F}} = \forall x (\underline{F}y \to (x \equiv 0 \vee x \equiv 1))$
- in this way, can transform entire formula $\phi \in L^{S_{ar}}$ into language of vector spaces

Remark. this section will discuss connection between a formula and its reletivization

(E) SYNTACTIC INTERPRETATIONS

Remark.
- in above examples (A)-(D), one structure spoke about another structure
  (A) in groups as S_g-structures about groups as S_{gr}-structures
  (B) in orderings as $\{<\}$-structures about orderings as $\{<, \leq\}$-structures
  (C) in rings about groups of units
  (D) in structures (eg vector space) about substructures whose domains are given by a unary relation symbol (eg scalar fields)
- a syntactic interpretation of a symbol set S' in a symbol set S will allow us to talk in S-structures about induced S'-structures
- will use S-formula $\phi_{S'}(v_0)$ to define the domain of the S'-structure under consideration,
  and for each symbol in S', will give a S-formula describing it
- ntn: $\phi(v_0, \dots, v_{n-1})$ for $\phi \in L_n^S$ and $\phi(t_0, \dots, t_{n-1})$ for $\phi \frac{t_0 \dots t_{n-1}}{v_0 \dots v_{n-1}}$

Definition. A syntatic interpretation of S' in S is a map $I : S' \cup \{S'\} \to L^S$ where
$I(S')$ is a formula $\phi_{S'}(v_0) \in L_1^S$
$I(R)$ is a formula $\phi_R(v_0, \dots, v_{n-1}) \in L_n^S$ for n-ary

$R \in S'$
$I(f)$ is a formula $\phi_f(v_0,...,v_{n-1},v_n) \in L^S_{n+1}$ for n-ary $f \in S'$
$I(c)$ is a formula $\phi_c(v_0)$ for $c \in S'$

Example.
- in many applications one has $\phi_{S'}(v_0) = v_0 \equiv v_0$
- the following set Φ_I of S-sentences says that $\phi_{S'}$ defines the domain of an S'-structure
  $\Phi_I = \{\exists v_0 \phi_{S'}(v_0), \forall v_0...\forall v_{n-1}((\phi_{S'}(v_0) \wedge ... \wedge \phi_{S'}(v_{n-1})) \rightarrow \exists^{=1} v_n(\phi_{S'}(v_n) \wedge \phi_f(v_0,...,v_{n-1},v_n))), \exists^{=1} v_0(\phi_{S'}(v_n) \wedge \phi_c(v_0))\}$
  for $f, c \in S'$
- if $\phi_{S'} = v_0 \equiv v_0$ then Φ_I is equivalent (sets Φ, Ψ of S-sentences st $\mathrm{Mod}^S\Phi = \mathrm{Mod}^S\Psi$, in particular $\Phi \models \chi$ iff $\Psi \models \chi$ for all $\chi \in L^S$) to $\{\forall v_0...\forall v_{n-1}\exists^{=1} v_n \phi_f(v_0,...v_{n-1},v_n) | f \in S'$ n-ary$\} \cup \{\exists^{=1} v_0 \phi_c(v_0) | c \in S'\}$

Definition.
- For S-structure $\mathfrak{A}$ with $\mathfrak{A} \models \Phi_I$, define S'-structire $\mathfrak{A}^{-I}$ as follows:
  $A^{-I} := \{a \in A | \mathfrak{A} \models \phi_{S'}[a]\}$;
  for $R \in S'$ and $a_0,...,a_{n-1} \in A^{-I}$:
  $R^{A^{-I}} a_0...a_{n-1}$:iff $\mathfrak{A} \models \phi_R[a_0,...,a_{n-1}]$;
  for $f \in S'$ and $a_0,...,a_{n-1}, a \in A^{-I}$:
  $f^{A^{-I}}(a_0...a_{n-1}) = a$:iff $\mathfrak{A} \models \phi_f[a_0,...,a_{n-1},a]$;
  for $c \in S'$ and $a \in A^{-I}$: $c^{A^{-I}} = a$:iff $\mathfrak{A} \models \phi_c[a]$
- I is the identity on $R \in S \cap S'$ means $\phi_R = Rv_0...v_{n-1}$
  similarly for $f \in S'$ and $c \in S'$ if $\phi_f = fv_0...v_{n-1} \equiv v_n$ and $\phi_c = c \equiv v_0$, respectively

Claim. *Let $S \subset S'$, $\phi_{S'} = v_0 \equiv v_0$, and I is the identity on all symbols on S*
then $\mathfrak{A}^{-I}|S = \mathfrak{A}$ for all S-structures $\mathfrak{A}$ with $\mathfrak{A} \models \Phi_I$

Remark. now can talk in S-structures about induced S'-structures

Theorem. *(2.2)(Thm on syntactic interpretations) Let syntactic interpretation I of S' in S*
then to every $\psi \in L^{S'}$ one can associate a $\psi^I \in L^S$ with free(ψ) =free(ψ^I) st for all S-structures $\mathfrak{A}$ with $\mathfrak{A} \models \Phi_I$ and all assignments β in $\mathfrak{A}^{-I}$,
(*) $(\mathfrak{A}, \beta) \models \phi^I$
in particluar, for $\phi \in L_0^{S'}$, $(\mathfrak{A}^{-I}, \beta) \models \phi$

Remark. rest of section:
apply to (A)-(C)
proof of thm 2.2
apply to (D)

Example.
- (A) let syntactic interpretation I of S_{grp} in S_g (ntn: $x, y,...$ for $v_0, v_1,...$)
  $\phi_{S_{grp}}(x) := x \equiv x$, $\phi_\circ(x,y,z) := x \circ y \equiv z$, $\phi_{-1}(x,y) := \exists z)\forall uu \circ z \equiv u \wedge x \circ y \equiv z)$, $\phi_e(x) := \forall y y \circ x \equiv y$
  clm: let group (as S_g-structure) $\mathfrak{A} = (a \circ^A)$ with identity element e^A and inverse $^{-1^A}$
  then $\mathfrak{A}^{-I} = (A, \circ^A, ^{-1^A}, e^A)$ and for all $\phi \in L_0^{S_{grp}}$ we have $\mathfrak{A}^{-I} \models \phi$ iff $\mathfrak{A} \models \phi^I$ and $\Phi_{grp} \models \phi$ iff $\Phi_g \models \phi^I$
  pf: see book, similar to (B) below
- (B) define the syntactic interpretatino I of $S' = \{<, \leq\}$ in $S = \{<\}$ as follows:
  $\phi_{S'} := v_0 \equiv v_0$, $\phi_< := v_0 < v_1$, $\phi_\leq := (v_0 < v_1 \vee v_0 \equiv v_1)$
  Then Φ_I is equivalent to the empty set, and ϕ^I is a $\{<\}$-sentence for $\phi \in L_0^{\{<,\leq\}}$
  clm: $\Phi_{ord} \models \phi$ iff $\Phi_{ord} \models \phi^I$
  pf: see book, uses thm (2.2)
- (C) concerning the group of units, we choose syntactic interpretation I of S_{gr} in S_{ar}:
  $I(S_{gr}) := \epsilon(x)$; $I(\circ) := x \cdot y = z$
  then Φ_I is equivalent to $\{\exists x \epsilon(x), \forall x \forall y(\epsilon(x) \wedge \epsilon(y) \rightarrow \epsilon(x \cdot y))\}$
  concerning a ring $\mathfrak{A}$ we have $\mathfrak{A} \models \Phi_I$ and $\mathfrak{A}^{-I} = \mathfrak{E}(\mathfrak{A})$.
  for $\phi \in L_0^{S_{gr}}$, the equivalence (*) says $\mathfrak{E}(\mathfrak{A}) \models \phi$ iff $\mathfrak{A} \models \phi^I$, which is the claim ($\circ$) in (C) (if we set $\phi' := \phi^I$)

Proof. (of 2.2)

Example. for (D), want to apply (2.2) to connect a formula and its relativization
Let $S = S' \cup \{P\}$
Define syntactic interpretation I of S' in S as the indentity on the symbols from S' and $\phi_{S'}(v_0) := Pv_0$
Then Φ_I is equivalent to
$\{\exists v_0 Pv_0\} \cup \{Pc | c \in S'\} \cup \{\forall v_0...\forall v_{n-1}(Pv_0 \wedge ... \wedge Pv_{n-1} \rightarrow Pfv_0...v_{n-1} | f \in S')\}$
and for an S-structure $(\mathfrak{A}, P^A)$ we have
(+) $(\mathfrak{A}, P^A) \models \Phi_I$ iff P^A is S'-closed in $\mathfrak{A}$
(++) if P^A is S'-closed in $\mathfrak{A}$ then $(\mathfrak{A}, P^{-I}) = [P^A]^\mathfrak{A}$
(recall (cp III.5) S-closed subset S of S-structure $\mathfrak{A}$. $[X]^\mathfrak{A}$ is the substructure of $\mathfrak{A}$ with domain X)
ntn: if $\psi \in L^{S'}$, write ψ^P for ψ^I and say "ψ is the reletivization of ψ to P"

Lemma. *(2.3)(Relativization Lemma)*
let $\mathfrak{A}$ be an $S \cup \{P\}$-structure st $P \notin S$ and P is unary
Suppose $P^A \subset A$ is S-closed in $\mathfrak{A}$.
then for $\psi \in L_0^S$, $[P^S]^\mathfrak{A} \models \psi$ iff $\mathfrak{A} \models \psi^P$
ie the relativizatin ϕ^P says in $\mathfrak{A}$ the same as ψ does in $[P^A]^\mathfrak{A}$

Proof. use (+) and (++), and note P^A being S-closed implies that it is $S \cup \{P\}$-closed
for direct proof, define for $\psi \in L^S$ the formula $\psi^P \in L^{S \cup \{P\}}$ inductively, then prove by induction on formulas

8.3. EXTENSIONS BY DEFINITIONS.

Example.
- in previous section, dealt with two axiom systems eg Φ_g and Φ_{grp}
  perhaps we only want to deal with one
- recall (VII.3) we extended $S = \{\in\}$ by the defined symbols $\emptyset, \cap, \cup, ...$
  will analyze these "extensions by definition"

Definition. (3.1)
let Φ a set of S-sentences
a) a S-definition of relation symbol $P \notin S$ in Φ is $\forall v_0...\forall v_{n-1}(Pv_0...v_{n-1} \leftrightarrow \phi_P(v_0,...,v_{n-1}))$ where $\phi_P(v_0,...,v_{n-1})$ an S-formula
b) a S-definition of function symbol of $f \notin S$ in Φ is
  $\forall v_0...\forall v_n(fv_0...v_{n-1} \equiv v_n \leftrightarrow \phi_f(v_0,...,v_{n-1},v_n))$ where $\phi_f(v_0,...,v_{n-1},v_n)$ an S-formula
  provided $\Phi \models \forall v_0...\forall v_{n-1}\exists^{=1} v_n \phi_f(v_0,...,v_n)$
c) An S-definition of consant symbol $c \notin S$ in Φ is $\forall v_0(c \equiv v_0 \leftrightarrow \phi_c(v_0))$ where $\phi_c(v_0)$ an S-formula
  provided $\Phi \models \exists^{=1} v_0 \phi_c(v_0)$

Example.
- note $\Phi_g \models \exists^{=1} x \forall y y \circ x \equiv y$
  so $\delta_e := \forall x(e \equiv x \leftrightarrow \forall y y \circ x \equiv y)$ is a S_g-definition of e in Φ_g
  so new symbol set $S_{gr} = \{\circ, e\}$ and new axiom system ("extension by definition") $\Phi_g \cup \{\delta_e\}$
  clm: S_{gr}-sentence sets $\Phi_g \cup \{\delta_e\}$ and Φ_{gr} are equivalent
- $\forall x \forall y(x \leq y \leftrightarrow (x < y \vee x \equiv y))$
  is a $\{<\}$-definition of $\leq$ in Φ_{ord}
- $\forall x \forall y \forall z(x \cap y \equiv z \leftrightarrow \forall w(w \in z \leftrightarrow (w \in x \wedge w \in y)))$
  is an $\{\in\}$-definition of $\cap$ in ZFC

Claim. *there were no major changes in transition from L^{S_g} to $L^{S_{gr}}$*
more precisely:
(E1) "extensions by def are conservative":
for all $\phi \in L_0^{S_g}$: $\Phi_g \cup \{\delta_e\} \models \phi$ iff $\Phi_g \models \phi$
(ie adding defs does not increase the set of provable sentences)
(E2) "Defined symbols can be eliminated":
for syntactic interpretation I of S_{gr} in S_g with $\phi_{S_{gr}}(x) := x \equiv x$, $\phi_\circ(x,y,z) := x \circ y = z$, $\phi_e(x) := \forall y y \circ x \equiv y$
the following holds for all $\chi \in L^{S_{gr}}$: $\Phi_g \cup \{\delta_e\} \models \chi \leftrightarrow \chi^I$
(E3) "the elimination of defined symbols respects the theory":
for I as in (E2) and $\phi \in L_0^{S_{gr}}$: $\Phi_g \cup \{\delta_e\} \models \phi$ iff $\Phi_g \models \phi^I$

Proof. (E3) follows from (E1),(E2) (see book).
(E1),(E2) follow from the "thm on defs" below.

Definition.
- Fix S. Let $s \notin S$ be a new relation, function, or const symbol.
  Let $\Phi \subset L_0^S$ and let δ_s be an S-definition of s in Φ
  define the associated syntactic interpretation I of $S' := S \cup \{s\}$ in S to be the identity on symbols from S and $(I(S') =)\phi_{S'}(v_0) := v_0 \equiv v_0$, $I(s) := \phi_s$ where ϕ_s is as in def 3.1

Claim. *keep ntn form above def*
Φ_I is logically equiv to
- *the empty set of sentences, if s is a relation symbol*
- *$\{\forall v_0...\forall v_{n-1}\exists^{=1} v_n \phi_f(v_0,...,v_{n-1},v_n)\}$ if s is function symbol f*
- *$\{\exists^{=1} v_0 \phi_c(v_0)\}$ if s is const c*

so for every S-structure $\mathfrak{A}$ with $\mathfrak{A} \models \Phi$:
(*) $\mathfrak{A} \models \Phi_I$
(**) $(\mathfrak{A}, s^A) \models \delta_s$ iff $\mathfrak{A}^{-I} = (\mathfrak{A}, s^A)$

Theorem. *(3.2)(Thm on definitions)*
Let Φ be S-formulas, $s \notin S$ a new symbol, δ_s a S-definition of s in Φ, and I the associated syntactic interpretation of $S \cup \{s\}$ in S.
then
a) for all $\phi \in L_0^S$, $\Phi \cup \{\delta_s\} \models \phi$ iff $\Phi \models \phi$
b) for all $\chi \in L_0^{S \cup \{s\}}$, $\Phi \cup \{\delta_s\} \models \chi \leftrightarrow \phi^I$
c) for all $\phi \in L_0^{S \cup \{s\}}$, $\Phi \cup \{\delta_s\} \models \phi$ iff $\Phi \models \phi^I$

Proof. see book

8.4. NORMAL FORMS.

Remark. this section: show that one can associate with every formula a logically equiv formula which has a special syntactic form

Definition. fix S, and let Φ S-formulas.
define $\langle\Phi\rangle$ to be the smallest subset of L^S containing Φ and containing with any formulas ϕ and χ the formulas $\neg\phi$ and $(\phi \vee \chi)$

Claim. $\Phi \subset L_r^S \Rightarrow \langle\Phi\rangle \subset L_r^S$

Lemma. *(4.1)*
Let $\Phi \subset L_r^S$.
Let $\mathfrak{A}, \mathfrak{B}$ S-structures, $a_0,...,a_{r-1} \in A$, $b_0,...,b_{r-1} \in B$
If
(*) $\mathfrak{A} \models \phi[a_0,...,a_{r-1}]$ iff $\mathfrak{B} \models \phi[b_0,...,b_{r-1}]$
holds for all $\phi \in \Phi$
then (*) holds for all $\phi \in \langle\Phi\rangle$

Proof. the set of ϕ for which (*) holds includes Φ and with ψ, χ also contains $\neg\psi, (\psi \vee \chi)$

Lemma. *(4.2)*
Let $\Phi = \{\phi_0,...,\phi_n\}$ be a finite set of formulas
Then every satisfiable formula in $\langle\Phi\rangle$ is logically equiv to a formula of the form
(+) $(\psi_{0,0} \wedge ... \wedge \psi_{o,n}) \vee ... \vee (\psi_{k,0} \wedge ... \wedge \psi_{k,n})$
where $k < 2^{n+1}$ and for $i \leq k$ and $j \leq n$, $\psi_{i,j} = \phi_j$

or $\psi_{i,j} = \neg\phi_j$
(ie a disjunction of conjuctions from $\{\phi_0, ..., \phi_n, \neg\phi_0, ..., \phi_n\}$*) in particular, there are only finitely many pairwise logically nonequivalent formulas in* $\langle\Phi\rangle$

Proof. long

Definition.
- a formula in disjuntive normal form is a formula which is a disjunction of conjunctions of atomic or negated atomic formulas
- quantifier-free formula contains no quantifiers

Theorem. *(thm on the disjunctive normal form)*
if ϕ *is quantifier-free*
then ϕ *is logically equiv to a formual in disjunctive normal form*

Proof. this is a cor to 4.2, short pf

Remark. will now consider formulas with quantifiers

Definition. formula ψ in prenex-normal form means it has the form $Q_0x_0...Q_{m-1}x_{m-1}\phi_0$ where $Q_i = \exists$ or $Q_i = \forall$ for $i < m$ and ϕ_0 is qunatifier-free.
then ψ has prefix $Q_0x_0...Q_{m-1}x_{m-1}$ and matrix ϕ_0

Theorem. *(thm on the prenex normal form)*
Every formula ϕ *is logically equivalent to a formula* ψ *in prenex normal form with free*(ϕ) *=free*(ψ)

Proof. long

Definition.
- formuals ϕ and ψ are equivalent for satisfaction means Satϕ iff Satψ
- formula ψ can be chosen univeral means its prenex normal prefix contains only universal quantifiers

Remark. next weaken the thm on prenex normal form condition of logcal equivalence to $\psi \models \phi$ and equivalence for satisfiction
then the formula can be chosen universal

Example. let $S = \{R\}$ and let S-formaula $\phi := \forall x\exists yRxy$
set $S' = \{R, f\}$ and let $\psi := \forall xRxfx$
Then ψ is universal and $\psi \models \phi$
ie each model of ψ is a model of ϕ
on the other hand, let $(A, R^A) \models \forall x\exists yRxy$
we have an interpretation R^A of R ie for every $a \in A$, an element $b \in A$ st R^Aab
choose an interpretation f^A of f st $R^Aaf^A(a)$ for all $a \in A$
then $(A, R^A, f^A) \models \forall xRxfx$ so $\forall xRxfx$ has a model.

Theorem. *(4.5)(thm on the skolem normal form)*
To each formula ϕ *one can associate a universal formula* ψ *in prenex normal form with* $\psi \models \phi$ *and free*(ϕ) *=free*(ψ) *st* ϕ, ψ *are equivalent for satisfaction*
Besides the symbols from ϕ*, the formula* ψ *may contain additional function symbols or consts*

Proof. long

9. EXTENSIONS OF FIRST-ORDER LOGIC

Remark.
- recall, the following cannot be characterized in the first-order language corresponding to them: structure $\mathfrak{N}$, the field of real numbers, and the class of torsion groups
- ch VII: can overcome this weakness by introducing a system of axioms for set theory in a first-order language, eg ZFC, which is sufficient for math, and within this system, carry out the arguments which are required, say, for a definition and characterization of $\mathfrak{N}$
- can also consider other languages with more expressive power, eg second-order language where we can directly characterize the natural numbers with Peano's axioms
- need to set up the semantics, prove correctness of inference rules, etc
- might want to apply more expressive language as a tool in math
  analogous to (VI.4) using the compactness thm in algebraic investigations

9.1. SECOND-ORDER LANGUAGE.

Remark. unlike first-order languages, second order languages can quantify over second-order objects (eg subsets)

Definition. (1.1, 1.2)
- Let symbol set S be just like first-order
  ie {relation, function, and const symbols}
- Let second-order alphabet contain the symbols of first-order alphabet, and for each $n \geq 1$, ctbly many n-ary relation variables $V_0^n, V_1^n, V_2^n, ...$ (ntn: $X, Y, ...$)
- set L_{II}^S of second-order S-formulas is generated by second-order calclulus of first-order rules extended by the rules
  a) if X is an n-ary relation variable and $t_1, ..., t_n$ are S-terms, then $Xt_1...t_n$ is an S-formula
  b) let S-formula ϕ and relation variable X, then $\exists X\phi$ is an S-formula
- A second-order assignment γ wrt structure $\mathfrak{A}$ is a map which takes variables v_i to elements of A and relation variables V_i^n to n-ary relations on A
- A second-order interpretation is $\mathfrak{I} = (\mathfrak{A}, \gamma)$
- second-order satisfaction relation is like first-order and
  a') $\mathfrak{I} \models Xt_1...t_n$:iff $\gamma(X)$ holds for $\mathfrak{I}(t_1), ..., \mathfrak{I}(t_n)$
  b') for n-ary X: $\mathfrak{I} \models \exists X\phi$:iff there is a $C \subset A^n$ st $\mathfrak{I}\frac{C}{X} \models \phi$ (where $\mathfrak{I}\frac{C}{X} = (\mathfrak{A}, \gamma\frac{C}{X})$ and $\gamma\frac{C}{X}$ agrees with γ and maps X to C)
- second-order logic $\mathcal{L}_{II}$ is the logical system (cf XIII.1) given by the languages L_{II}^S together with the satisfaction relation for these languages
  ntn: $\mathcal{L}_I$ denotes first-order logic

Remark. (1.2)
- define free occurences of variables and relation variables similary
  define L_{II}^S−sentence to be a formula without free variables or free relation variables
- can prove the analogue of the coincidence lemma
- ntn: if ϕ is an L_{II}^S-sentence, can write $\mathfrak{A} \models \phi$
- let $\forall X\phi$ be an abbreviation for $\neg\exists X\neg\phi$
  then $\mathfrak{I} \models \forall X^n\phi$:iff for all $C \subset A^n$: $\mathfrak{I}\frac{C}{X} \models \phi$
- Peano's axioms (cf III.7.3) are $L_{II}^{\{\sigma,0\}}$-sentences, for X a unary relation variable
  (P1) $\forall x\neg\sigma x \equiv 0$
  (P2) $\forall x\forall y(\sigma x \equiv \sigma y \to x \equiv y)$
  (P3) $\forall X((X0 \wedge \forall x(Xx \to X\sigma x)) \to \forall xXy)$
  note: unlike first-order axioms, second-order axioms can characterize (up to ismoprhism) the structure $(\mathbb{N}, \sigma, 0)$
- the ordered field $\mathfrak{R}^<$, is the only (up to isomprhism) completely ordered field
  Let $\psi_{\mathfrak{R}^<} := \Phi_{ofd} \cup \{\chi\}$ where Φ_{ofd} is in (III.6.5) and χ is second-order S_{ar}-sentence "every nonempty set which is bdd above has a supremum" (see book for long sentence)
  then for $S_{ar}^<$-structure $\mathfrak{A}$, $\mathfrak{A} \models \psi_{\mathfrak{R}^<}$ iff $\mathfrak{A} \cong \mathfrak{R}^<$
- let S arbitrary. The following L_{II}^S sentence is valid
  (+) $\forall x\forall y(x \equiv y \leftrightarrow \forall X(Xx \leftrightarrow Xy))$
  this is Liebniz's *identitas indescernibilium* (two things are equal precicely when there is no property which distinguishes them)
  so could have excluded the equality symbol and used this instead
- could have included function variables which can also be quantified
  easier to read, but this does not increase expressive power
  ex (cf VIII.1) eliminate of function variable symbol
  see book for sentence $\phi :=$"every injective function is surjective" (note: iff finite) with function variable symbols
  see book for sentence ϕ_{fin} with no function variable symbol but has the same models as ϕ
- can define operations such as substitution and relativization analogously to first-order logic
- can verify various semantic properties such as analogue of ismorphism lemma
  but cant verify other semantic properties such as completeness thm, compactness thm, or Lowenheim-Skolem thm

Theorem. *(1.4) The compactness thm does not hold for* $\mathcal{L}_{II}$

Proof. counterexample: set of sentences $\{\phi_{fin}\} \cup \{\phi_{\geq n} | n \geq 2\}$ is not satisfiable, but any finite subset is

Theorem. *(1.5)*
The Lowenheim-Skolem thm does not hold for $\mathcal{L}_{II}$

Proof. counterexample with sentences that say "A is ctble", "A is unctble"

Claim. *(1.6)*
for $\mathcal{L}_{II}$*, there is no correct and complete system of derivation rules*

Proof. otherwise, could prove compactness thm in same way as for $\mathcal{L}_I$

Remark.
- can still set up correct rules
- eg take first-order rules and add rules for quantification over relation variables
  $\frac{\Gamma \quad \phi}{\Gamma \quad \exists X\phi}$; $\frac{\Gamma \quad \phi \quad \psi}{\Gamma \quad \exists X\phi \quad \psi}$ if X is not free in $\Gamma\psi$
- these rules are largely sufficient for the purposes of math
- second-order language provides more convenient formulation of math
- the expressive power of second-order languages is so great that several properties of first-order language dont hold.
  lacking these properties, second-order logic not as useful in mathematical applications
- set theory, eg based on ZFC, is not sufficient to decide basic semantic questions in $\mathcal{L}_{II}$.
  pf: recall ZFC is not sufficient to prove or prove the negation of Cantor's continuum hypothesis CH (for every $A \subset \mathbb{R}$, either A is at most ctble, or there is a bijection of $\mathbb{R}$ onto A) nor its negation can be proved in ZFC (cf VII.3)
  see book for formalization of CH in second-order language
  the validity of this formalization can neither be established or refuted in ZFC

9.2. THE SYSTEM $\mathcal{L}_{\omega_1\omega}$.

Remark. extend first-order logic with a "formula" with infinite disjunctions
allows characterization of the class of torsion groups

todo

9.3. **THE SYSTEM $\mathcal{L}_Q$.**

Remark. extend first-order logic with quantifier Q where formula $Qx\phi$ says "there are unctbly many x satisfying ϕ"

todo

10. LIMITATIONS OF THE FORMAL METHOD

Remark. syntactically, operations of sequent rules is mechanical operations on symbol strings

Example. group theory axioms $\Phi_{gr} = \{\phi_0, \phi_1, \phi_2\}$
completeness thm $\Rightarrow$ for all S_{gr}-sentences ϕ, $\Phi_{gr} \models \phi$ iff $\Phi_{gr} \vdash \phi$
so ϕ is a thm of group theory iff sequent $\phi_0\phi_1\phi_2\phi$ is derivable
define $Th_{gr} := \{\psi \in L_0^{S_{gr}} | \Phi_{gr} \models \psi\}$

Remark. can generate theory (eg Th_{gr}) by systematically applying all sequent rules to generate all possible derivations and add sentence $\phi \in L_0^{S_{gr}}$ if one arrives at a derivation whose last sequent is $\phi_0\phi_1\phi_2\phi$
ie there is a mechanical procedure to list all theorems in Th_{gr} (although infeasible since derivations and sequents are arbitrarily long)

Definition. enumerable set can be listed by a "procedure"

Remark.
- an enumeration "procedure" can yield many trivialities eg $\forall x(x \equiv x \to x \equiv x)$
- dont know when the procedure will yield a useful thm
- a group theorist is only interested in specific statements ψ ie want to determine whether $\psi \in Th_{gr}$
- strategy: either proof of ψ or counterexample (ie find a group $\mathfrak{G}$ st $\mathfrak{G} \models \neg\phi$)
  it is often difficult to do either of these
- question: is there a procedure which can be applied to arbitrary S_{gr}-sentences and decides in finitely many steps whether it belongs to Th_{gr}?

Definition. decidable theory means there exists such a "procedure"

Remark. this chapter:
§1: informal
§2: formalize decidablility and enumerability using register machine (these are topics in recursion theory ("theory of computability"))
rest of chapter: applications to first and second-order logic

10.1. DECIDABILITY AND ENUMERABILITY.

(A) PROCEDURES, DECIDABILITY

Example.
- deciding primality
  input: $n \in \mathbb{N}$
  output: "yes" if prime, "no" if not
  procedure: if $n = 0$ or 1, then "no"
  if $n \geq 2$, test whether $2, ..., n-1$ divides n
  if yes, output "yes", if no, output "no"
- multiply two numbers
  input: $n, m \in \mathbb{N}$
  output: $n \cdot m$
  procedure:
- compute square root
  imput: $n \in \mathbb{N}$
  output: $\sqrt{n}$ or $\lfloor\sqrt{n}\rfloor$
  procedure:
- list the primes in increasing order
  input: none
  output: list of primes
  procedure: generate successively $n = 1, 2, 3, ...$, check each using prime test above, print if prime

Remark. commonalities of above "procedures" ("effective procedures", "process", "algorithm", "program (description of procedure)")
- proceed step-by-step
- operate on symbol strings
- can be carried out by a reliably programmed computer
- can stop after finitely many steps and yield an output or run without ever stopping

Definition. Let alphabet $\mathcal{A}$, set $W \subset \mathcal{A}^*$ ie a "set of words over $\mathcal{A}$"
$\mathfrak{P}$ a decision "procedure" for W if for every input $\zeta \in \mathcal{A}^*$, $\mathfrak{P}$ eventually stops, having previously given exactly one output $\eta \in \mathcal{A}^*$, where $\eta = \square$ (empty word) if $\zeta \in W$ and $\eta \neq \square$ if $\zeta \notin W$
ie $\mathfrak{P}$ answers "$\zeta \in W$?" in finitely many steps
W is decidable if exists decision procedure

Example. deciding primality above
$\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, W = set of primes in decimal expansion

Claim. *T^S is decidable*

Proof. (sketch)
eg let S_∞, $\mathcal{A}_\infty = \{v_0, v_1, ..., \neg, \vee, \exists, \equiv,), (\} \cup S_\infty$
given: $\zeta \in \mathcal{A}_\infty^*$
find length $l(\zeta)$
if $l(\zeta) = 0$, then ζ not a term
if $l(\zeta) = 1$, then ζ is term iff variable or const
if $l(\zeta) > 0$, then if doesnt begin with a function symbol then not term
if does begin with a function symbol, say $\zeta = f\zeta'$ where f n-ary
then if ζ' decomposable (using this procedure) into terms $\zeta_1, ..., \zeta_n$, then ζ is a term, else not
note: each ζ_i shorter than ζ so will obtain answer in finitely many steps

Claim. *L^S is decidable*

Proof. similar

Remark. might want finite alphabet
define $\mathcal{A}_0 := \{v, \underline{0}, ..., \underline{9}, \overline{0}, ..., \overline{0}, \neg, \vee, \exists,), (\} \cup \{R, f, c\}$
now can represent symbols in $\mathcal{A}$ (eg $\mathcal{A}_\infty$) as symbols in $\mathcal{A}_0$ eg R_2^3 represented $R\underline{2}\overline{3}$

(B) ENUMERABILITY

Example. listing the primes, see above

Definition. let alphabet $\mathcal{A}$, $W \subset \mathcal{A}^*$
$\mathfrak{P}$ is a enumeration "procedure" for W if $\mathfrak{P}$ eventually yields, as output, exactly the words in W
note: in any order, possibly with repetition
W enumerable means exists procedure

Claim. *if alphabet $\mathcal{A}$ finite then $\mathcal{A}^*$ is enumerable*

Proof. Let $\mathcal{A} := \{a_0, a_1, ..., a_n\}$
define lexicographical order on $\mathcal{A}^*$ st ζ precedes ζ' if either
a) $l(\zeta) < l(\zeta')$ or
b) $l(\zeta) = l(\zeta')$ and ζ precedes ζ' in dictionary (there are $a_i, a_j \in \mathcal{A}$ with $i < j$ st $\zeta = \xi a_i \eta$ and $\zeta' = \xi a_j \eta'$ where $\xi, \eta, \eta' \in \mathcal{A}^*$)
eg $\mathcal{A}$ = {a,b,c,...,z}, then "zuu" precedes "papa" precedes "papi" ie ordering begins as $\square, a_0, ..., a_n, a_0a_0, a_0a_1, ..., a_1a_0, ..., a_na_n, ...$
let $\mathfrak{P}$ enumerate $\mathcal{A}^*$ in lexicographic order

Claim. *$\{\phi \in L_0^{S\infty} | \models \phi\}$ is enumerable*

Proof. same as enumerating $\{\phi \in L_0^{S\infty} | \vdash \phi\}$ since completeness
list this set similar to Th_{gr}
(ie construct the first n terms and formulas in lexicogrpahical order, form the finitely many derivations of length $\leq n$ using only those n formulas and terms, and which contain sequents that containt $\leq n$ members, and if last sequent is sentence ϕ, then print it. Then move to $n+1$)

(C) THE RELATIONSHIP BETWEEN ENUMERABILITY AND DECIDABILITY

Remark. given enumerable set, can try to check if decidable by listing all elements and waiting for a particular one
but dont know if/when it will appear

Theorem. *every decidable set is enumerable*

Proof. let $\mathfrak{P}$ decide $W \in \mathcal{A}^*$
list $\mathcal{A}^*$ in lexicographical order and check each element with $\mathfrak{P}$, and if so, print it

Theorem. *$W \subset \mathcal{A}^*$ is decidable iff W and its complement $\mathcal{A}^* \setminus W$ are eumerable*

Proof. ($\Rightarrow$) let W decidable
then so is $\mathcal{A}^* \setminus W$ by switching decision "yes" and "no"
then both are enumerable by previous thm
($\Leftarrow$) let W and $\mathcal{A}^* \setminus W$ enumerable
simultaneously enumerate W and $\mathcal{A}^* \setminus W$ until given ζ is yielded by one of them

Remark. defs for decidable and enumerable dont need fixed alphabet, see exercise

(D) COMPUTABLE FUNCTIONS

Definition. Let $\mathcal{A}, \mathcal{B}$ alphabets
function from $\mathcal{A}^*$ to $\mathcal{B}^*$ is determined by a "procedure" for which each input from $\mathcal{A}^*$ yields a word in $\mathcal{B}^*$
a computable function can have its values computed in this way

Example. length function l assigns to each word in $\mathcal{A}^*$ its length in decimal notation as a word over $\{0, 1, ..., 9\}$

Remark. can define function and enumerablilty/decidability from each other

10.2. REGISTER MACHINES.

Remark.
- our intuitive notion of "procedures" does not enable us to prove that a particular set is not decidable (unless we show that every possible procedure is not a decision procedure)
- want to formalize "procedure"
- will define a programming languege
  will define "procedure" to be exactly those procedures which can be programmed in this language
- A. Turing first introduced a similar concept

Definition. fix alphabet $\mathcal{A} = \{a_0, ..., a_r\}$
- register machine is a computer where programs are executed
  have memory units $R_0, ..., R_m$ called registers
  st at each stage of the computation, every register contains a word from $\mathcal{A}^*$
  note: assume arbitrarily many registers, each can store arbitrary length word
- a program over $\mathcal{A}$ consists of instructions each beginning with a label $n \in \mathbb{N}$ and 5 instructions permitted
  1) L LET $R_i = R_i + a_j$ for $L, i, j \in \mathbb{N}$, $j \leq r$
     (add instruction: add letter a_j to the end of the word in register R_i)

2) L LET $R_i = R_i - a_j$ for $L, i, j \in \mathbb{N}$, $j \leq r$
(subtraction instruction: if the word in register R_i ends in the letter a_j, delete this a_j, otherwise leave the word unchanged)
3) L IF $R_i = \square$ THEN L' ELSE L_0 OR ... OR L_r for $L, i, L', L_0, ..., L_r \in \mathbb{N}$
(jump instruction: if the word in register R_i contains the empty word, go to instruction labeled L'
if the word in register R_i ends with a_0 (resp $a_1, ..., a_r$), go to instruction labeled L_0 (resp. $L_1, ..., L_r$))
4) L PRINT for $L \in \mathbb{N}$
(print instruction: print as output the word stored in R_0)
5) L HALT for $L \in \mathbb{N}$
(halt instruction: halt)

- a register program ("program") is a finite sequence $\alpha_0, ..., \alpha_k$ of instructions of the form (1)-(5) st
(i) α_i has label $i \in \{0, 1, ..., k\}$
(ii) every jump instruction refers to lables $\leq k$
(iii) only the last line α_k is the halt instruction

Claim. *each program P gives rise to a procedure*

Proof. let a computer with all registers occuring in P
at the beginning of execution, register R_0 contains the input (possibly empty) and all other registers contain empty string
each step of computation corresponds to one instruction of P
start with first instruction, proceed to next instruction or jump if instruction 3
print register R_0 at every print instruction
stop when halt is reached

Example. Program to check evenness of input
see book

Definition.
- program P is started with word $\zeta \in \mathcal{A}^*$ if P begins the computation with ζ in R_0 and $\square$ in the remaining registers
- P: $\zeta \rightarrow$halt means P started with ζ and eventually halted
P: $\zeta \rightarrow \infty$ means P started with ζ and doesnt halt
- P: $\zeta \rightarrow \eta$, $\zeta, \eta \in \mathcal{A}^*$, means P started with ζ, gave one output η and halted

Example. P: $\zeta \rightarrow \infty$, see book

Remark. ntn: instruction L GOTO L' means L if $R_0 = \square$ THEN L' ELSE L' OR ... OR L'

Example. P: $\zeta \rightarrow \zeta\zeta$
see book, long

Remark. now can formally define decidability and enumerability

Definition. Let $W \subset \mathcal{A}^*$
- program P decides W if for all $\zeta \in \mathcal{A}^*$
P: $\zeta \rightarrow \square$ if $\zeta \in W$
P: $\zeta \rightarrow \eta$, $\eta \neq \square$ if $\zeta \notin W$
- W is register-decidable ("R-decidable") if there is a program which decides W
- program P enumerates W if P, started with $\square$, prints out exactly the words in W (in any order, possibly with repetitions)
- W is register-enumerable ("R-enumerable") if there is a program which enumerates W

Example.
- above program to check evenness shows that $\mathbb{N}$ is decidable
- if P enumerates an infinite set, then P: $\square \rightarrow \infty$
- example above with P: $\zeta \rightarrow \infty$ shows that $W = \{\square, a_0, a_0a_0, ...\}$ is R-enumerable
- the progarm 0 HALT enumerates the empty set
- see book for another program that enumerates the empty set

Definition. Let alphabets $\mathcal{A}, \mathcal{B}$, $F : \mathcal{A}^* \rightarrow \mathcal{B}^*$
program P over $\mathcal{A} \cup \mathcal{B}$ computes F if for all $\zeta \in \mathcal{A}^*$, P: $\zeta \rightarrow F(\zeta)$
F is register-computable ("R-computable") if there is a program over $\mathcal{A} \cup \mathcal{B}$ which computes F

Example. example above with P: $\zeta \rightarrow \zeta\zeta$ computes the function $F : \{a_0, a_1\}^* \rightarrow \{a_0, a_1\}^*$ with $F(\zeta) = \zeta\zeta$

Remark.
- previous formalization defs can be extended to n-ary relations and functions
eg a program to compute a binary function has inputs in the first two registers
- a program decides a procedure
so R-decidable $\Rightarrow$ decidable and similarly with enumerable and computable
- how about converses? ie can any procedure be simulated by a program?
cant treat mathematically since "procedure" is just an intuitive concept
- Church-Turing thesis: every procedure can be simlated by a program (so the converses hold)

Definition. recursive refers to R-decidable sets and R-computable functions
recursively enumerable refers to R-enumerable sets

Remark. in proofs for R-enumerability and R-decidablility, we avoid writing register programs and just give intuitive procedure since Church-Turing thesis

10.3. THE HALTING PROBLEM FOR REGISTER MACHINES.

Remark.
- fix alphabet $\mathcal{A} = \{a_0, ..., a_r\}$
- goal: present register programs over $\mathcal{A}$ suitably coded as words over $\mathcal{A}$ ie associate every P over $\mathcal{A}$ with a word $\xi_P \in \mathcal{A}^*$
Will show that this subset of $\mathcal{A}^*$ is not R-decidable

Definition.
- alphabet $\mathcal{B} := \mathcal{A} \cup \{A,B,C,...,X,Y,Z\} \cup \{0, 1, ..., 9\} \cup \{=, \cdot, +, \square, \S\}$
- Godel numbering of programs over $\mathcal{A}$ with words over $\{a_0\}^*$
represent a program P over $\mathcal{A}$ with a word over $\mathcal{B}$
eg 0LETR1=R1-a_0§1PRINT§2HALT
say this is the nth word in the lexicographic ordering of $\mathcal{B}^*$
define $\xi_P = \underbrace{a_0...a_0}_{n\text{-times}}$ as the Godel number of P
- $\Pi := \{\xi_P | \text{P is a program over } \mathcal{A}\}$
- effective means can program in register machine

Claim. *for each P, can effectively determine $\xi_P \in \mathcal{A}^*$*
conversely, for each $\xi_P \in \Pi$, can effectively determine program P

Lemma. Π *is R-decidable*

Remark. following thm presents first examples of R-undecidable sets

Theorem. *(3.2)(undecidablility of the halting problem)*
a) $\Pi'_{halt} := \{\xi_P\}P$ is a program over $\mathcal{A}$ and P: $\xi_P \rightarrow halt\}$ is not R-decidable
b) $\Pi_{halt} := \{\xi_P\}P$ is a program over $\mathcal{A}$ and P: $\square \rightarrow halt\}$ is not R-decidable

Proof. long, see book
a) uses diagonal argument
b) uses a?

Claim. *undecidablility of halting problem does not depend on our particular choice of Godel numbering*

Proof. the only properties of map P$\mapsto \xi_P$ used in the pf was injectively and effectiveness

Remark. thm 3.2 decides the halting question "uniformly" for each P
but there are particular programs P which you can decide whether they halt or not

Lemma. Π_{halt} *is R-enumerable*

Proof. book, short

Corollary. $\mathcal{A}^* \setminus \Pi_{halt}$ *is not R-enumerable*

Proof. apply earlier thm about sets and their complements being R-enumerable

Remark.
- so Π_{halt} is an example of R-enumerable but not R-decidable
- rest of section: costs of computations, P vs NP

Definition. see (XI.4) for precise def of propositional logic
- propositional formulas are built, using $\neg, \vee$, from propositional variables $p_0, p_1, ...$ like first-order formulas are built from atomic formulas.
- satisfiable propositional formula means one can assign truth values T,F to propositional variables st the whole formula is T

Claim. *the set SAT of satisfiable propositional formulas is decidable*

Proof. if propositional variables in formula α are among $p_0, .., p_n$
so check α for the finite number of possible truth assignmetns to $p_0, ..., p_n$
eg n propositional variables has 2^n possible truth assignments

Remark.
- but 2^{1000} may take longer than a human lifetime so SAT is "theoretically" decidable, but not "practically" decidable
- complexity theory studies number of computation steps and memory use (in the registers)
- will consider time complexity

Definition.
- a register program P over $\mathcal{A}$ is t-bounded in time means that P, started with word $\zeta \in \mathcal{A}^*$ of length n, stops after at most $t(n)$ steps
- program P is polynomially bounded in time means it is t-bounded in time for a suitable polynomial t with coefs in $\mathbb{N}$
- define $\mathcal{P}$ to be the class of R-decidable sets which can be decided by a program in polynomially bounded time
- $\mathcal{NP}$ is the class of sets of non-deterministic (usual instructions and instructions L GOTO $\mathfrak{Z}$, where $\mathfrak{Z}$ is a nonempty finite set of labels, ie randomly chooses a label in $\mathfrak{Z}$) polynomially bounded in time register programs

Remark. Church's (or Cobham and Edmonds) thesis of practical computability:
"practically decidable" sets are identified with the sets in $\mathcal{P}$
note: this is not realistic since high degree polynomials might take life-times

Remark.
- $\Pi \subset \mathcal{P}$
- it is not know whether the sets PRIM (decimal representions of all primes) or SAT are in $\mathcal{P}$
- it is conjectured that $PRIM \in \mathcal{P}$ and $SAT \notin \mathcal{P}$
- SAT$\in \mathcal{NP}$
- $\mathcal{P} \subset \mathcal{NP}$, by def

- SAT$\notin \mathcal{P} \Rightarrow \mathcal{P} \neq \mathcal{NP}$, but the hypothesis is unknown

10.4. **THE UNDECIDABILITY OF FIRST-ORDER LOGIC.**

Remark. recall the set of valid first-order S_∞ sentences is enumerable
how about decidable?

Theorem. *(undecidability of first-order logic)*
the set $\{\phi \in L_0^{S\infty} | \models \phi\}$ of valid S_∞-sentences is not R-decidable

Proof. reduce to the halting problem
very long, see book

10.5. **TRAHTENBROT'S THM AND THE INCOMPLETENESS OF SECOND-ORDER LOGIC.** todo

10.6. **THEORIES AND DECIDABILITY.**

Remark.
- this section:
  - enumerability and decidability wrt theories
  - prove undecidability of arithmetic
- assume symbol set S effectively given

(A) FIRST ORDER THEORIES

Definition.
- theory $T \subset L_0^S$ means it is satisifiable and closed under consequence (every S-sentence which follows form T already belongs to T)
- $Th(\mathfrak{A}) := \{\phi \in L_0^S : \mathfrak{A} \models \phi\}$ is the theory of S-structure $\mathfrak{A}$; a theory
- arithmetic is $Th(\mathfrak{N})$ where S_{ar}-structure $\mathfrak{N} = \{\mathbb{N}, +, \cdot, 0, 1\}$
- $\Phi^\models := \{\phi \in L_0^S | \Phi \models \phi\}$, where $\Phi \subset L_0^S$

Claim.
- *if T is a theory, then $T = T^\models$*
- *if Φ is satisfiable set of S-sentences then $\Phi^\models$ is a theory*

Example.
- $\emptyset^\models = \{\phi \in L_0^S | \models \phi\}$
- Let $S = S_{gr}$. $Th_{gr} = \Phi_{gr}^\models$ is group theory
- Let $S = \{\in\}$. $Th_{ZFC} := ZFC^\models$ is ZFC set theory
- Let $S = S_{ar}$. $Th_{PA} := \Phi_{PA}^\models$ is (first-order) Peano arithmetic
  recall Φ_{PA} was given in III.7.5 but there was one second-order induction axiom, and have infinitely many first-order induction axioms
  $\Phi_{PA} := \{ \forall x \neg x + 1 \equiv 0,$
  $\forall x \forall y (x + 1 \equiv y + 1 \to x \equiv y)$
  $\forall x x + 0 \equiv x, \forall x \forall y (x + (y + 1) \equiv (x + y + 1)$
  $\forall x x \cdot 0 \equiv 0, \forall x \forall y (x \cdot (y + 1) \equiv x \cdot + x$
  for all $x_1, ..., x_n, y$ and all $\phi \in L^{S_{ar}}$ st free$(\phi) \subset \{x_1, ..., x_n, y\}$, the sentence
  $\forall x_1 ... \forall x_n ((\phi_y^0 \wedge \forall y (\phi \to \phi_y^{y+1})) \to \forall y \phi)\}$

Claim.
- $\Phi_{PA}^\models \subset Th(\mathfrak{N})$ *since $\mathfrak{N}$ is a model of Φ_{PA}*
- *many thms (sentences) in $Th(\mathfrak{N})$ can be derived from Φ_{PA}*
  but not all sentences in $Th(\mathfrak{N})$ are derivable from Φ_{PA}
  pf: cor to big thm later in this section

Definition.
- Theory T is R-axiomatizable means there is an R-decidable set Φ of sentences st $T = \Phi^\models$
- Theory T is finitely axiomatizable means there is a finite set Φ of sentences st $T = \Phi^\models$

Claim.
- *every finitely axiomatizable theory can be axiomatized by a single sentence*
  pf: conjunction of axioms
- *finitely axiomatizable $\Rightarrow$ R-axiomatizable*
- *theories Th_{PA} and Th_{ZFC} are R-axiomatizable but not finitely axiomatizable (will show later)*

Theorem. *Theory is R-axiomatizable $\Rightarrow$ R-enumerable*

Proof. generate systematically all derivable sequents
using decision procedure for axioms, decide whether antecedent are axioms
if so, list the succedent

Claim. *R-axiomatizable theory need not be R-decidable*

Proof. eg $T = \emptyset^\models$
eg $T = T_{gr}$

Remark. situation is different if T is complete

Definition. Theory $T \in L_0^S$ is complete means for every S-sentence ϕ we have either $\phi \in T$ or $\neg\phi \in T$

Claim. $Th(\mathfrak{A})$ *is complete for each structure $\mathfrak{A}$*

Theorem. *(6.5)*
a) every R-axiomatizable complete theory is R-decidable
b) every R-enumerable complete theory is R-decidable

Proof. a) follows from (b) since R-axiomatizable $\Rightarrow$ R-enumerable
b) given ϕ, enumerate T until ϕ or $\neg\phi$ is listed
if ϕ is listed, print "yes", if $\neg\phi$ is listed, print "no"

Remark. to show an axiomatizable theory is decidable, can show completeness
where methods to show completeness in ex 6.7 and ch XII

(B) THE UNDECIDABILITY OF ARITHMETIC

Remark.
- want to prove that arithmetic is undecidable
  ie cant decide whether arbitrary S_{ar}-sentence holds in $\mathfrak{N}$
- proof of thm uses a lemma
  proof of lem uses another lem
  will state lems once their context is initiated

Lemma. *(6.8)*
with any given program P, can effectively associate an S_{ar}-formula $\chi_P(v_0, ..., v_{2n+2})$ st for all $l_0, ..., l_0, L, m_0, ..., m_n \in \mathbb{N}$, the following holds
$\mathfrak{N} \models \chi_P[l_0, ..., l_n, L, m_0, ..., m_n]$ *iff P, beginning with config $(0, l_0, ..., l_n)$, after finitely many steps, reaches config $(L, m_0, ..., m_n)$*

Proof. later

Theorem. *(6.9)(undecidability of arithmetic)*
Arithmetic, ie $Th(\mathfrak{N})$, is not R-decidable

Proof. will effectively assign to each register program P over $\mathcal{A} = \{|\}$ an S_{ar}-sentence ϕ_P st $\mathfrak{N} \models \phi_P$ iff P: $\square \to$halt
then undecidability of $Th(\mathfrak{N})$ follows form undecidability of Π_{halt}
to define ϕ_P, will need formula χ_P which, in $\mathfrak{N}$, describes how P operates; a lem will give us formula χ_P
Let k st instructions in P are $\alpha_0, ..., \alpha_k$
Let n be st registers in P are $R_1, ..., R_n$
Recall a configuration of P is $(n + 2)$-tuple $(L, m_0, .., m_n)$ (where L corresponds to α_L to be executed, and $m_0, ..., m_n$ are the contents of the registers) of natural numbers where $L \leq k$
using lem 6.8, define $\phi_p := \exists v_{2n+2} \chi_p(0, ..., 0, k, v_{n+2}, ..., v_{2n+2})$
ntn: $\phi(n, m)$ stands for $\phi_{\frac{nm}{v_0 v_1}}$
ntn: 1,2,..., stands for 1,1+1,...
$\mathfrak{N} \models \phi_P$ iff P begins with config $(0, ..., 0)$ and after finitely many steps reaches config $(k, m_0, ..., m_n)$ where α_k is halt
iff P: $\square \to$halt

Corollary. *(6.10)*
$Th(\mathfrak{N})$ is neither R-axiomatizable nor R-enumerable
in particular, $\Phi_{PA}^\models$ is a proper subset of $Th(\mathfrak{N})$

Proof. follows form $Th(\mathfrak{N})$ complete and 6.5 (how?)

Remark. so $Th(\mathfrak{N})$ is not amenable to purely "mechanical" treatment
ie cant systematically prove all true arithmetial sentences
cant decide, enumerate, axiomatize $Th(\mathfrak{N})$

Proof. of lem 6.8, but need...

Lemma. *(6.11)(Godel's β-function lem)*
there is a function $\beta : \mathbb{N}^3 \to \mathbb{N}$ with properties:
a) for every sequence $(a_0, ..., a_r)$ over $\mathbb{N}$ there exist $t, p \in \mathbb{N}$ st for all $i \leq r$, $\beta(t, p, i) = a_i$
b) β is definable in $L^{S_{ar}}$
ie there exists an S_{ar} formula $\phi_\beta(v_0, v_1, v_2, v_3)$ st for all $t, p, i, a \in \mathbb{N}$, $\mathfrak{N} \models \phi[t, p, i, a]$ iff $\beta(t, p, i) = a$

Proof. number theory

Proof. finish 6.8

Remark. next, another consequence of the fact that computations of register machines can be described in $\mathfrak{N}$

Theorem. *(6.12)*
let $r \geq 1$
a) given a r-ary R-decidable relation $\mathfrak{Q}$ over $\mathbb{N}$, there is an S_{ar}-formula $\phi(v_0, ..., v_{r-1})$ st for all $l_0, ..., l_{r-1} \in \mathbb{N}$,
$\mathfrak{Q}(_{;0}, ..., l_{r-1}$ iff $\mathfrak{N} \models \phi(l_0, ..., l_{r-1})$
b) given a R-computable function $f : \mathbb{N}^r \to \mathbb{N}$, there is an S_{ar}-formula $\phi(v_0, ..., v_{r-1}, v_r)$ st for all $l_0, ..., l_{r-1}, l_r \in \mathbb{N}$,
$f(l_0, ..., l_{r-1}) = l_r$ iff $\mathfrak{N} \models \phi(l_0, ..., l_{r-1}, l_r)$
in particular, $\mathfrak{N} \models \exists^{=1} v_r \phi(l_0, ..., l_{r-1}, v_r)$

Proof. long

Definition. arithmetical functions and relations are functions and relations over $\mathbb{N}$ which can be described by an S_{ar}-formula
so 6.12 $\Rightarrow$ all R-decidable relations and R-computable functions over $\mathbb{N}$ are arithmetical

Remark. the thm on the undecidablility of arithmetic has been strengthened
1970: Matijasevic proved that set PIR (polynomials in integer coefficients with integer roots (cf 1.11)) is not R-decidable
see book for more

10.7. SELF-REFERENTIAL STATEMENTS AND GODEL'S INCOMPLETENESS THMS.

Remark.
- Godel proved that arithmetic is not R-axiomatizable using another method:
  within sufficiently strong axiom systems there are self-referential formulas (make statements about themselves)
- this section: use self-referential formulas to find limitations of the formal method
  will conduct arguments on the syntactic level
  assume $\Phi \subset L_0^{S_{ar}}$

Definition. (7.1)
- relation $\mathfrak{Q} \subset \mathbb{N}^r$ is representable in Φ means there is an S_{ar}-formula $\phi(v_0, ..., v_{r-1})$ st for all $n_0, ..., n_{r-1} \in \mathbb{N}$:
  if $\mathfrak{Q} n_0 ... n_{r-1}$ then $\Phi \vdash \phi(n_0, ..., n_{r-1})$
  if not $\mathfrak{Q} n_0 ... n_{r-1}$ then $\Phi \vdash \neg\phi(n_0, ..., n_{r-1})$
  ie $\phi(v_0, ..., v_{r-1})$ represents $\mathfrak{Q}$ in Φ
- function $F : \mathbb{N}^r \to \mathbb{N}$ is representable in Φ means there is an S_{ar}-formula $\phi(v_0, ..., v_{r-1}, v_r)$ st for all $n_0, ..., n_{r-1}, n_r \in \mathbb{N}$:
  if $F(n_0 ... n_{r-1}) = n_r$ then $\Phi \vdash \phi(n_0, ..., n_{r-1}, n_r)$
  if $F(n_0 ... n_{r-1}) \neq n_r$ then $\Phi \vdash \neg\phi(n_0, ..., n_{r-1}, n_r)$
  $\Phi \vdash \exists^{=1} v_r \phi(n_0, ..., n_{r-1}, v_r)$
  ie $\phi(v_0, ..., v_{r-1})$ represents $\mathfrak{Q}$ in Φ

Lemma. *(7.2)*
a) if Φ is inconsistent then every relation over $\mathbb{N}$ and every function over $\mathbb{N}$ is representable in Φ
b) if $\Phi \subset \Phi' \subset L_0^{S_{ar}}$ then the relations and functions representable in Φ are also representable in Φ'
c) Let ConΦ. If Φ is R-decidable then every relation representable in Φ is R-decidable and every function representable in Φ is R-computable

Proof.

Definition. Φ allows representations means all R-decidable relations and all R-computable functions over $\mathbb{N}$ are representable in Φ
intuition: Φ is rich enough to describe how procedures operate

Theorem. *(7.3)*
$Th(\mathfrak{N})$ allows representations

Proof. note: for every S_{ar}-sentence ϕ, ($\mathfrak{N} \models \phi$ iff $Th(\mathfrak{N}) \models \phi$) and (not $\mathfrak{N} \models \phi$ iff $Th(\mathfrak{N}) \models \neg\phi$) then immidiate from 6.12

Theorem. *(7.4)*
Φ_{PA} allows representations

Proof. not given, suggests looking at considerations leading to 6.12

Remark.
- assume that a surjective Godel numbering of S_{ar}-formulas is effectively given
  ie every number is the Godel number of some formula
  ntn: n^ϕ is the Godel number of ϕ
- key to construct self-referential formulas: translate statements about formulas into arithmetical statements
  eg a statement about the derivability of ϕ becomes an arithmetical statement about n^ϕ, which can be formalized as an S_{ar}-sentence
- will proceed analogously to the (self-referential) liar paradox ("I am not telling the truth now" can either be true or false, if true then it is false, and if false then it is true)
- next, show that within a sufficiently rich (ie allows representations) system, every property which is expressible in the system gives rise to a self-referential sentence

Theorem. *(7.5)(Fixed-point thm)*
Suppose Φ allows representations.
then for every $\psi \in L_1^{S_{ar}}$, there is an S_{ar}-sentence ϕ st $\Phi \vdash \phi \leftrightarrow \psi(n^\phi)$
intuition: ϕ says "I have property ψ"

Proof. book

Remark. next thm: in a system Φ rich enough (consistent, allows representations), one cannot speak about the truth of all its statements
intuition: "true" statements correspond to sentences in $\Phi^\vdash = \{\phi \in L_0^{S_{ar}}\}$, and to say that one can speak of "truth" or "falsity" in Φ is to say that $\Phi^\vdash$ (more precisely $\{n^\phi | \phi \in \Phi^\vdash\}$) is representable in Φ

Lemma. *(7.6)*
Let Φ consistent and allows representations
Then $\Phi^\vdash$ is not representable in Φ

Proof. book, short

Remark. 7.6 has implications for semantics and syntactics (see following two thms)

Theorem. *(7.7)(Tarski's thm)*
a) suppose Φ consistent, allows representations then $\Phi^\models$ is not representable in Φ
b) $Th(\mathfrak{N})$ is not representable in $Th(\mathfrak{N})$
ie "there is no truth definition for arithmetic within arithmetic"

Proof. a) completeness, 7.6
b) special case of (a)

Theorem. *(7.8)(Godel's First Incompleteness thm)*
Let Φ consistent, R-decidable, allows representations
then there is an S_{ar}-sentence ϕ st neither $\Phi \vdash \phi$ nor $\Phi \vdash \neg\phi$

Proof. by contradiction, suppose that for every S_{ar}-sentence ϕ, $\Phi \vdash \phi$ or $\Phi \vdash \neg\phi$
then $\Phi^\vdash$ is comlete, hence R-decidable (cf 6.5)
thus, since Φ allows representatins, $\Phi^\vdash$ is representable in Φ
contradicts 7.6

Remark.
- next, refine above to result concerning the consistency of mathematics
  ie will show Godel's second incompleteness thm: the consistency of a sufficiently rich system cannot be proved using only the means available within the system
- in the following, assume $\Phi \subset L_0^{S_{ar}}$ decidable and allow representations

Definition. choose an effective enumeration of all derivations in the sequent calculus associated with S_{ar}
define a relation H by
Hnm iff the mth derivation ends with a sequent of the form $\psi_0 ... \psi_{k-1} \phi$ where $\psi_0, ..., \psi_{k-1} \in \Phi$ and $n = n^\phi$

Claim.
- *since Φ is decidable, so is H*
- *$\Phi \vdash \phi$ iff there is $m \in \mathbb{N}$ st $Hn^\phi m$*
- *since Φ allows representations, H can be represented in Φ by a suitable formula $\phi_H(v_0, v_1) \in L_2^{S_{ar}}$*

Definition.
- set $\mathrm{Der}_\Phi(x) := \exists y \phi_H(x, y)$
- define ϕ: for $\psi = \neg\mathrm{Der}_\Phi(x)$, choose with 7.5 a fixed point $\phi \in L_0^{S_{ar}}$
  ie an S_{ar}-sentence ϕ with
  (*) $\Phi \vdash \phi \leftrightarrow \neg\mathrm{Der}_\Phi(n^\phi)$
  intuitively, ϕ says "I am not provable from Φ"

Lemma. *(7.9)*
if ConΦ then not $\Phi \vdash \phi$

Proof. suppose $\Phi \vdash \phi$.
Choose m st $Hn^\phi m$.
Then $\Phi \vdash \phi_H(n^\phi, m)$
Then $\Phi \vdash \mathrm{Der}_\Phi(n^{\neg 0 \equiv 0}$
hence IncΦ

Definition. S_{ar}-sentence $\mathrm{Consis}_\Phi := \neg\mathrm{Der}_\Phi(n^{\neg 0 \equiv 0})$

Claim.
- *$Consis_\Phi$ expresses the consistency of Φ since $\Phi \vdash 0 \equiv 0$ implies (ConΦ iff not $\Phi \vdash \neg 0 \equiv 0$)*
- *reformulate lem 7.9*
  (**) $Consis_\Phi \to \neg Der_\Phi(n^\phi)$
  pf: (tedious so not given) but can carry out on the basis of Φ
  ie can show $\Phi \vdash Consis_\Phi \to \neg Der_\Phi(n^\phi)$ in case $\Phi \supset \Phi_{PA}$ (see ex 7.12 for specific $\phi_H(x, y)$ in Der_Φ)

Theorem. *(7.10)(Godel's second incompleteness thm)*
Let Φ consistent and R-decidable with $\Phi \supset \Phi_{PA}$ then not $\Phi \vdash Consis_\Phi$

Proof. if $\Phi \vdash \mathrm{Consis}_\Phi$ then (***) implies $\Phi \vdash \neg\mathrm{Der}_\Phi(n^\phi)$.
(*) implies $\Phi \vdash \phi$
contradiction to (7.9)

Remark.
- for $\Phi = \Phi_{PA}$, the consistency of Φ_{PA} cannot be proved n the basis of Φ_{PA}
- So Hilbert's program (to prove consistency of Φ_{PA} in basis of Φ_{PA}) cannot be carried out in its original form
- can transfer above arguments to other systems where there is a substitute for natural numbers and where R-decidable relations and R-computable functions are representable
  in particular, it applies to ZFC (cf VIII.3)

Theorem. *(7.11)*
if Con ZFC then not ZFC$\vdash Consis_{ZFC}$
where $Consis_{ZFC}$ is a $\{\in\}$-sentence expressing consistency of ZFC

Remark.
- so if math is consistent, we cant prove its consistency by mathematical means
- can similarly transfer Tarski's thm and Godel's first incompleteness thm to set theory
- transferred 7.8: for every decidable and consistent system Φ of axioms for set theory which contains ZFC, there is a $\{\in\}$-sentence ϕ st neither $\Phi \vdash \phi$ nor $\Phi \vdash \neg\phi$.
  intuitively, there is no decidable consistent system of axioms for math which, for every math statement, allows us to either prove or disprove it
  this is an inherent limitation of the axiomatic method
- refurmulate 7.11 using Matijesevic's result mentioned last section:
  One can write down a polynomial p in finitely many indeterminates with integer coefs for which the following holds: Math is consistent iff p has no integer root
  by 7.11: if p has no root, then math cannot prove it