Theorems

Negation, inequivalence, and false

(3.11)		$\neg p \equiv q \equiv p \equiv \neg q$
(3.14)		$(p \not\equiv q) \equiv \neg p \equiv q$
(3.15)		$(\neg p \equiv p \equiv false)$
(3.18)	Mutual Associativity	$((p \not\equiv q) \equiv r) \equiv (p \not\equiv (q \equiv r))$
(3.19)	Mutual interchangeability	$p \not\equiv q \equiv r \equiv p \equiv q \not\equiv r$

Disjunction

(3.27)	Axiom, Distributivity of $\vee$ over $\equiv$	$p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$
(3.28)	Axiom, Excluded Middle	$p \vee \neg p$
(3.31)	Distributivity of $\vee$ over $\vee$	$p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$
(3.32)		$p \vee q \equiv p \vee \neg q \equiv p$

Conjunction

(3.35)	Axiom, Golden rule	$p \wedge q \equiv p \equiv q \equiv p \vee q$
(3.41)	Distributivity of $\wedge$ over $\wedge$	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$
(3.43)	Absorption	(a) $p \wedge (p \vee q) \equiv p$ (b) $p \vee (p \wedge q) \equiv p$
(3.44)	Absorption	(a) $p \wedge (\neg p \vee q) \equiv p \wedge q$ (b) $p \vee (\neg p \wedge q) \equiv p \vee q$
(3.47)	De Morgan	(a) $\neg(p \wedge q) \equiv \neg p \vee \neg q$ (b) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
(3.48)		$p \wedge q \equiv p \wedge \neg q \equiv \neg p$
(3.49)		$p \wedge (q \equiv r) \equiv p \wedge q \equiv p \wedge r \equiv p$
(3.50)		$p \wedge (q \equiv p) \equiv p \wedge q$
(3.51)	Replacement	$(p \equiv q) \wedge (r \equiv p) \equiv (p \equiv q) \vee (r \equiv q)$
(3.52)	Definition of $\equiv$	$p \equiv q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
(3.53)	Exclusive or	$p \not\equiv q \equiv (\neg p \wedge q) \vee (p \wedge \neg q)$
(3.55)		$(p \wedge q) \wedge r \equiv p \equiv q \equiv r$ $\equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r$

Implication

(3.57)	Axiom, Def of $\Rightarrow$	$p \Rightarrow q \equiv p \vee q \equiv q$
(3.59)		$p \Rightarrow q \equiv \neg p \vee q$
(3.60)		$p \Rightarrow q \equiv p \wedge q \equiv p$
(3.61)	Contrapositive	$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$
(3.62)		$p \Rightarrow (q \equiv r) \equiv p \wedge q \equiv p \wedge r$
(3.63)	Distr. of $\Rightarrow$ over $\equiv$	$p \Rightarrow (q \equiv r) \equiv p \Rightarrow q \equiv p \Rightarrow r$
(3.64)		$p \Rightarrow (q \Rightarrow r) \equiv (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$
(3.65)	Shunting	$p \wedge q \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r)$
(3.66)		$p \wedge (p \Rightarrow q) \equiv p \wedge q$
(3.67)		$p \wedge (q \Rightarrow p) \equiv p$
(3.68)		$p \vee (p \Rightarrow q) \equiv true$
(3.69)		$p \vee (q \Rightarrow p) \equiv q \Rightarrow p$
(3.70)		$p \vee q \Rightarrow p \wedge q \equiv p \equiv q$
(3.71)	Reflexivity of $\Rightarrow$	$p \Rightarrow p \equiv true$
(3.72)	Right zero of $\Rightarrow$	$p \Rightarrow true \equiv true$
(3.73)	Left identity of $\Rightarrow$	$true \Rightarrow p \equiv p$
(3.74)		$p \Rightarrow false \equiv \neg p$
(3.75)		$false \Rightarrow p \equiv true$
(3.76)	Weakening/strengthening	(a) $p \Rightarrow p \vee q$ (b) $p \wedge q \Rightarrow p$ (c) $p \wedge q \Rightarrow p \vee q$ (d) $p \vee (q \wedge r) \Rightarrow p \vee q$ (e) $p \wedge q \Rightarrow p \wedge (q \vee r)$
(3.77)	Modus ponens	$p \wedge (p \Rightarrow q) \Rightarrow q$
(3.78)		$(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q \Rightarrow r)$
(3.79)		$(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \equiv r$
(3.80)	Mutual implication	$(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \equiv q)$
(3.81)	Antisymmetry	$(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow (p \equiv q)$
(3.82)	Transitivity	(a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$ (b) $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$ (c) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$

General Laws of Quantification

For symmetric and associative binary operator $\star$ with identity u.

(8.13)	**Axiom, Empty range:** $(\star x \mid false : P) = u$
(8.14)	**Axiom, One-point rule:** Provided $\neg occurs(`x', `E')$, $(\star x \mid x = E : P) = P[x := E]$
(8.15)	**Axiom, Distributivity:** Provided each quantification is defined, $(\star x \mid R : P) \star (\star x \mid R : Q) = (\star x \mid R : P \star Q)$
(8.16)	**Axiom, Range split:** Provided $R \wedge S \equiv false$ and each quantification is defined, $(\star x \mid R \vee S : P) = (\star x \mid R \wedge S : P) = (\star x \mid R : P) \star (\star X \mid S : P)$
(8.17)	**Axiom, Range split:** Provided each quantification is defined, $(\star x \mid R \vee S : P) \star (\star x \mid R \wedge S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$
(8.18)	**Axiom, Range split for idempotent $\star$:** Prov. each quant. is defined, $(\star x \mid R \vee S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$
(8.19)	**Axiom, Interchange of dummies:** Provided each quantification is defined, $\neg occurs(`y', `R')$, and $\neg occurs(`x', `Q')$, $(\star x \mid R : (\star y \mid Q : P)) = (\star y \mid Q : (\star x \mid R : P))$
(8.20)	**Axiom, Nesting:** Provided $\neg occurs(`y', `R')$, $(\star x, y \mid R \wedge Q : P) = (\star x \mid R : (\star y \mid Q : P))$
(8.21)	**Axiom, Dummy renaming:** Provided $\neg occurs(`y', `R, P')$, $(\star x \mid R : P) = (\star y \mid R[x := y] : P[x := y])$
(8.22)	**Change of dummy:** Provided $\neg occurs(`y', `R, P')$, and f has an inverse, $(\star x \mid R : P) = (\star y \mid R[x := f.y] : P[x := f.y])$
(8.23)	**Split off term:** $(\star i \mid 0 \le i < n+1 : P) = (\star i \mid 0 \le i < n : P) \star P_n^i$

Theorems of the Predicate Calculus

Universal quantification

(9.2)	**Axiom, Trading:**	$(\forall x \mid R : P) \equiv (\forall x \mid : R \Rightarrow P)$
(9.3)	**Trading:**	(a) $(\forall x \mid R : P) \equiv (\forall x \mid : \neg R \vee P)$ (b) $(\forall x \mid R : P) \equiv (\forall x \mid : R \wedge P \equiv R)$ (c) $(\forall x \mid R : P) \equiv (\forall x \mid : R \vee P \equiv P)$
(9.4)	**Trading:**	(a) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \Rightarrow P)$ (b) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : \neg R \vee P)$ (c) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \wedge P \equiv R)$ (d) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \vee P \equiv P)$
(9.5)	**Axiom, Distributivity of $\vee$ over $\forall$:**	Prov. $\neg occurs(`x', `P')$, $P \vee (\forall x \mid R : Q) \equiv (\forall x \mid R : P \vee Q)$
(9.6)		Provided $\neg occurs(`x', `P')$, $(\forall x \mid R : P) \equiv P \vee (\forall x \mid : \neg R)$
(9.7)	**Distributivity of $\wedge$ over $\forall$:**	Provided $\neg occurs(`x', `P')$, $\neg(\forall x \mid : \neg R) \Rightarrow ((\forall x \mid R : P \wedge Q) \equiv P \wedge (\forall x \mid R : Q))$
(9.8)		$(\forall x \mid R : true) \equiv true$
(9.9)		$(\forall x \mid R : P \equiv Q) \Rightarrow ((\forall x \mid R : P) \equiv (\forall x \mid R : Q))$
(9.10)	**Range weakening/strengthening:**	$(\forall x \mid Q \vee R : P) \Rightarrow (\forall x \mid Q : P)$
(9.11)	**Body weakening/strengthening:**	$(\forall x \mid R : P \wedge Q) \Rightarrow (\forall x \mid R : P)$
(9.12)	**Monotonicity of $\forall$:**	$(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P))$
(9.13)	**Instantiation:**	$(\forall x \mid : P) \Rightarrow P[x := e]$
(9.16)		P is a theorem iff $(\forall x \mid : P)$ is a theorem.

Existential quantification

(9.17)	**Axiom, Generalized De Morgan:**	$(\exists x \mid R : P) \equiv \neg(\forall x \mid R : \neg P)$
(9.18)	**Generalized De Morgan:**	(a) $\neg(\exists x \mid R : \neg P) \equiv (\forall x \mid R : P)$ (b) $\neg(\exists x \mid R : P) \equiv (\forall x \mid R : \neg P)$ (c) $(\exists x \mid R : \neg P) \equiv \neg(\forall x \mid R : P)$
(9.19)	**Trading:**	$(\exists x \mid R : P) \equiv (\exists x \mid : R \wedge P)$
(9.20)	**Trading:**	$(\exists \mid Q \wedge R : P) \equiv (\exists x \mid Q : R \wedge P)$
(9.21)	**Distributivity of $\wedge$ over $\exists$:**	Provided $\neg occurs(`x', `P')$, $P \wedge (\exists x \mid R : Q) \equiv (\exists x \mid R : P \wedge Q)$
(9.22)		$(\exists x \mid R : false) \equiv false$
(9.23)	**Distributivity of $\vee$ over $\exists$:**	Provided $\neg occurs(`x', `P')$, $(\equiv x \mid : R) \Rightarrow ((\equiv x \mid R : P \vee Q) \equiv P \vee (\exists x \mid R : Q))$
(9.24)		$(\exists x \mid R : false) \equiv false$
(9.25)	**Range weakening/strengthening:**	$(\exists x \mid R : P) \Rightarrow (\exists x \mid Q \vee R : P)$
(9.26)	**Body weakening/strengthening:**	$(\exists x \mid R : P) \Rightarrow (\exists x \mid R : P \vee Q)$
(9.27)	**Monotonicity of $\exists$:**	$(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P))$
(9.28)	**$\exists$-Introduction:**	$P[x := E] \Rightarrow (\exists x \mid : P)$
(9.29)	**Interchange of quantifications:**	Provided $\neg occurs(`y', `R')$ and $\neg occurs(`x', `Q')$, $(\exists x \mid R : (\forall y \mid Q : P)) \Rightarrow (\forall y \mid Q : (\exists x \mid R : P))$
(9.30)		Provided $\neg occurs(`\hat{x}', `Q')$, $(\exists x \mid R : P) \Rightarrow Q$ is a theorem iff $(R \wedge P)[x := \hat{x}] \Rightarrow Q$ is a theorem

Conditional Statements

(10.5) Proof method for IF: To prove $\{Q\}IF\{R\}$, prove $\{Q \wedge B\}S1\{R\}$ and $\{Q \wedge \neg B\}S2\{R\}$

Find precondition

Given $\{?\}S\{R\}$. To find ? textual sub S into R

Set Theory

(11.3)	**Axiom, Set membership:**	Provided $\neg occurs(`x', `F')$, $F \in x \mid R : E \equiv (\exists x \mid R : F = E)$
(11.4)	**Axiom, Extensionality:**	$S = T \equiv (\forall x \mid: x \in S \equiv x \in T)$
(11.5)		$S = \{x \mid x \in S : x\}$
(11.6)	Provided $\neg occurs(`y', `R')$ and $\neg occurs(`y', `E')$,	$\{x \mid R : E\} = \{y \mid (\exists x \mid R : y = E)\}$
(11.7)		$x \in \{x \mid R\} \equiv R$
(11.9)		$\{x \mid Q\} = \{x \mid R\} \equiv (\forall x \mid: Q \equiv R)$
(11.12)	**Axiom, Size:**	$\#S = (\sum x \mid x \in S : 1)$
(11.13)	**Axiom, Subset:**	$S \subseteq T \equiv (\forall x \mid x \in S : x \in T)$
(11.14)	**Axiom, Proper subset:**	$S \subset T \equiv S \subseteq T \ \wedge \ S \neq T$
(11.17)	**Axiom, Complement:**	$v \in \sim S \equiv v \in \mathbf{U} \wedge v \notin S$
(11.18)		$v \in \sim S \equiv v \notin S$ (for v in $\mathbf{U}$)
(11.19)		$\sim\sim S = S$
(11.20)	**Axiom, Union:**	$v \in S \cup T \equiv v \in S \vee v \in T$
(11.21)	**Axiom, Intersection:**	$v \in S \cap T \equiv v \in S \wedge v \in T$
(11.22)	**Axiom, Difference:**	$v \in S - T \equiv v \in S \wedge v \notin T$
(11.23)	**Axiom, Power set:**	$v \in \mathcal{P}S \equiv v \subseteq S$
(11.24)	**Definition.** For E_s, a set expression, E_p, a predicate expression can be calculated:	$\emptyset \rightarrow false, \mathbf{U} \rightarrow true, \cup \rightarrow \vee, \cap \rightarrow \wedge, \sim \rightarrow \neg$
(11.25)	**Metatheorem.** For any set expressions E_s and F_s	$E_s = F_s \Leftrightarrow E_p \equiv F_p, E_s \subseteq F_s \Leftrightarrow E_p \Rightarrow F_p, E_s = \mathbf{U} \Leftrightarrow E_p \equiv true$

Properties of $\cup$

(11.26)	**Symmetry of $\cup$:**	$S \cup T = T \cup S$
(11.27)	**Associativity of $\cup$:**	$(S \cup T) \cup U = S \cup (T \cup U)$
(11.28)	**Idempotency of $\cup$:**	$S \cup S = S$
(11.29)	**Zero of $\cup$:**	$S \cup \mathbf{U} = \mathbf{U}$
(11.30)	**Identity of $\cup$:**	$S \cup \emptyset = S$
(11.31)	**Weakening:**	$S \subseteq S \cup T$
(11.32)	**Excluded middle:**	$S \cup \sim S = \mathbf{U}$

Properties of $\cap$

(11.33)	**Symmetry of $\cap$:**	$S \cap T = T \cap S$
(11.34)	**Associativity of $\cap$:**	$(S \cap T) \cap U = S \cap (T \cap U)$
(11.35)	**Idempotency of $\cap$:**	$S \cap S = S$
(11.36)	**Zero of $\cap$:**	$S \cap \emptyset = \emptyset$
(11.37)	**Identity of $\cap$:**	$S \cap \mathbf{U} = S$
(11.38)	**Strengthening:**	$S \cap T \subseteq S$
(11.38)	**Contradiction:**	$S \cap \sim S = \emptyset$

Additional Properties

(11.40)	**Distributivity of $\cup$ over $\cap$:**	$S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$
(11.41)	**Distributivity of $\cap$ over $\cup$:**	$S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$
(11.42)	**De Morgan:**	(a) $\sim (S \cup T) = \sim S \cap \sim T$
(11.57)	**Antisymmetry:**	$S \subseteq T \wedge T \subseteq S \equiv S = T$
(11.58)	**Reflexivity:**	$S \subseteq S$
(11.59)	**Transitivity:**	$S \subseteq T \wedge T \subseteq U \Rightarrow S \subseteq U$
(11.70)	**Transitivity**	(a) $S \subseteq T \wedge T \subset U \Rightarrow S \subset U$ (b) $S \subset T \wedge T \subseteq U \Rightarrow S \subset U$ (c) $S \subset T \wedge T \subset U \Rightarrow S \subset U$

(11.43)	$S \subseteq T \wedge U \subseteq V \Rightarrow (S \cup U) \subseteq (T \cup V)$	(11.44)	$S \subseteq T \wedge U \subseteq V \Rightarrow (S \cap U) \subseteq (T \cap V)$
(11.45)	$S \subseteq T \equiv S \cup T = T$	(11.46)	$S \subseteq T \equiv S \cap T = S$
(11.47)	$S \cup T = \mathbf{U} \equiv (\forall x \mid x \in \mathbf{U} : x \notin S \Rightarrow x \in T)$	(11.48)	$S \cap T = \emptyset \equiv (\forall x \mid: x \in S \Rightarrow x \notin T)$
(11.49)	$S - T = S \cap \sim T$	(11.50)	$S - T \subseteq S$
(11.54)	$S-(T \cup U) = (S-T) \cap (S-U)$	(11.52)	$S \cap (T - S) = \emptyset$
(11.56)	$(\forall x \mid: P \Rightarrow Q) \equiv \{x \mid P\} \subseteq \{x \mid Q\}$	(11.62)	$S \subset T \equiv S \subseteq T \wedge (\exists x \mid x \in T : x \notin S)$
(11.61)	$S \subset T \equiv S \subseteq T \wedge \neg(T \subseteq S)$	(11.53)	$S \cup (T - S) = S \cup T$
(11.55)	$S-(T \cap U) = (S-T) \cup (S-U)$	(11.60)	$\emptyset \subseteq S$
(11.51)	$S - \emptyset = S$	(11.63)	$S \subseteq T \equiv S \subset T \vee S = T$
(11.64)	$S \not\subset S$	(11.65)	$S \subset T \Rightarrow S \subseteq T$
(11.66)	$S \subset T \Rightarrow T \not\subseteq S$	(11.67)	$S \subseteq T \Rightarrow T \not\subset S$
(11.68)	$S \subseteq T \wedge \neg(U \subseteq T) \Rightarrow \neg(U \subseteq S)$	(11.69a)	$(\exists x \mid x \in S : x \notin T) \Rightarrow S \neq T$
(11.69b)	$S \subset T \wedge T \subseteq U \Rightarrow S \subset U$	(11.69c)	$S \subset T \wedge T \subset U \Rightarrow S \subset U$

Induction

(12.3)	**Axiom, Mathematical Induction over $\mathbb{N}$:**	$(\forall n : \mathbb{N} \mid: (\forall i \mid 0 \le i < n : P.i) \Rightarrow P.n) \Rightarrow (\forall n : N \mid: P.n)$
(12.4)	**Mathematical Induction over $\mathbb{N}$:**	$(\forall n : \mathbb{N} \mid: (\forall i \mid 0 \le i < n : P.i) \Rightarrow P.n) \equiv (\forall n : \mathbb{N} \mid: P.n)$
(12.15)	**properties of golden ratio:**	$\phi^2 = \phi + 1 \& \hat{\phi}^2 = \hat{\phi} + 1$

Correctness of loops

(12.41)		**do** $B \rightarrow S$ **od**
(12.43)	**Fundamental invariance theorem**	Suppose $\{P \wedge B\}S\{P\}$ holds and $\{P\}$ **do** $B \rightarrow S$ **od** $\{true\}$, then $\{P\}$ **do** $B \rightarrow S$ **od** $\{P \wedge \neg B\}$ holds.
(12.45)	**Checklist**	(a) P is $true$ before the loop. Q $\Rightarrow$ P[S] (b) P is a loop invariant: $\{P \wedge B\}S\{P\}$ (c) Exe. of the loop terminates. P $\wedge$ B $\Rightarrow$ T > 0 (d) R holds upon termination: $P \wedge \neg B \Rightarrow R$

Tuples and cross-products

	Axiom, Cartesian product:	$S \times T = \{b, c \mid b \in S \wedge c \in T : (b, c)\}$
(14.4)	**Membership**	$\langle x, y \rangle \in S \times T \equiv x \in S \wedge y \in T$

Relations Functions

	$\langle b, c \rangle \in \rho$ and $b \rho c$ are interchangable
(14.5)	$\langle x, y \rangle \in S \times T \equiv \langle y, x \rangle \in T \times S$
(14.6)	$S = \Phi \Rightarrow S \times T = T \times S = \Phi$
(14.7)	$S \times T = T \times \equiv S = \Phi \vee T = \Phi \vee S = T$
(14.8)	**Dist of $\times$ over $\cup$:** $S \times (T \cup U) = (S \times T) \cup (S \times U)$ $(S \cup T) \times U = (S \times U) \cup (T \times U)$
(14.9)	**Dist of $\times$ over $\cap$:** $S \times (T \cap U) = (S \times T) \cap (S \times U)$ $(S \cap T) \times U = (S \times U) \cap (T \times U)$
(14.10)	**Dist of $\times$ over -:** $S \times (T - U) = (S \times T) - (S \times U)$
(14.11)	**Monotonicity:** $T \subseteq U \Rightarrow S \times T \subseteq S \times U$
(14.12)	$S \subseteq U \wedge T \subseteq V \Rightarrow S \times T \subseteq U \times V$
(14.14)	$(S \cap T) \times (U \cap V) = (S \times U) \cap (T \times V)$
(14.16)	$Dom.\rho = \{b : B \mid (\exists c \mid : b \rho c)\}$
(14.17)	$Ran.\rho = \{c : C \mid (\exists b \mid : b \rho c)\}$
(14.20)	$\langle b, d \rangle \in \rho \circ \sigma \equiv (\exists c \mid c \in C : \langle b, c \rangle \in \rho \wedge \langle c, d \rangle \in \sigma)$
(14.21)	$b(\rho \circ \sigma)d \equiv (\exists c \mid : b \ \rho \ c \ \sigma \ d)$
(14.22)	**Associativity of $\circ$:** $\rho \circ (\sigma \circ \theta) = (\rho \circ \sigma) \circ \theta$
(14.23)	**Dist of $\circ$ over $\cup$:** $\rho \circ (\sigma \cup \theta) = \rho \circ \sigma \cup \rho \circ \theta$ $(\sigma \cup \theta) \circ \rho = \sigma \circ \rho \cup \theta \circ \rho$
(14.24)	**Dist of $\circ$ over $\cap$:** $\rho \circ (\sigma \cap \theta) \subseteq \rho \circ \sigma \cap \rho \circ \theta$ $(\sigma \cap \theta) \circ \rho \subseteq \sigma \circ \rho \cap \theta \circ \rho$
(14.25)	$\rho^0 = i_B$ (the identity relation on B) $\rho^n + 1 = \rho^n \circ \rho$ (for $n \ge 0$)
(14.26)	$\rho^m \circ \rho^n = \rho^{m+n}$ (for $m \ge 0, n \ge 0$)
(14.27)	$(\rho^m)^n = \rho^{m.n}$ (for $m \ge 0, n \ge 0$)
(14.30)	Let ρ be a relation. $r(\rho)$ is a refliexive closure, $s(\rho)$ is the symmetric closure, ρ^+ is the transitive closure, and ρ^* is the refliexive transitive closure.
(14.39)	**Definition** for f and g $f \bullet g \equiv g \circ f$

Modern Algebra

- **Structure of Algebras**
  - An **algebra** has a set S, the **carrier**, and **operations** defined on that carrier.
  - **Signature** of an algebra is the name of carrier and the types of its operators.
  - Element 1 in S is a **left identity** of $\circ$ over S if $1 \circ b = b$ for all $b \in S$.
  - 1 is a **right identity** if $b \circ 1 = b$ for all $b \in S$.
  - 1 is an **identity** if it is both a left and right identity.
  - Zeroes and inverses are unique.
  - Def. Subset T of a set S is **closed** under an operator if applying operator to elements of T always produces a result in T.
  - Def. $\langle T, \Phi \rangle$ is a **subalgebra** of $\langle S, \Phi \rangle$ if T is closed under every operator in Φ.
  - Thrm. A subalgebra of a group is a group iff the inverse of every element of the subalgebra is in the subalgebra.
  - Thrm. A subalgebra of a finite group is a group.
  - Thrm. Let b be an element of a group $\langle S, \circ, 1 \rangle$.
  - Let set S_b cosist of all powers of b (including negative powers).
  - Then $\langle S_b, \circ, 1 \rangle$ is a subgroup of $\langle S, \circ, 1 \rangle$.
  - A function h is an **isomorphism** if it is one-to-one and onto,
    - each pair of nullary operators can be mapped to each other via h,
    - each pair of unary operators, $h(\sim b) = \hat{\sim} h.b$,
    - and each pair of binary operators, $h(b \circ c) = h.b \hat{\circ} h.c$.
  - A and $\hat{A}$ are **isomorphic** and $\hat{A}$ is called the **isomorphic image** of A.
- **Automorphism** is an isomorphism from A to A.
- **Homomorphism** is an isomorphism but h does not have to be one-to-one and/or onto.
- **Group Theory**
  - **Semigroup** is an algebra $\langle S, \circ \rangle$, where $\circ$ is a binary associative operator, and with no identity.
  - **Monoid** $\langle S, \circ, 1 \rangle$ is a semigroup with an identity 1.
  - **Submonoid** contains subset of S with the identity.
  - Any semigroup can be made into a monoid by adding an identity element.
  - A **group** is an algebra $(S, \circ, 1)$ in which
    1. $\circ$ is a binary, associative operator,
    2. 1 is an identity,
    3. and every element has an inverse.
  - A symmetric, commutative, or abelian group is an albelian monoid in which every element has an inverse.

Cancellation:	$b \circ d = c \circ d \equiv b = c$; $d \circ b = d \circ c \equiv b = c$
Unique solution:	$b \circ x = c \equiv x = b^{-1} \circ c$; $x \circ b = c \equiv x = c \circ b^{-1}$
One-to-one:	$b \neq c \equiv d \circ b \neq d \circ c$; $b \neq c \equiv b \circ d \neq c \circ d$
Onto:	$(\exists x \mid: b \circ x = c)$; $(\exists x \mid: x \circ b = c)$

$b^0 = 1$	$b^n = b^{n-1} \circ b$
$b^m \circ b^n = b^{m+n}$	$b^{-n} = (b^{-1})^n$
$(b^m)^n = b^{m \cdot n}$	$b^n = b^p \equiv b^n - p = 1$

Order of element b in group with identity 1 is the least positive integer m such that $b^m = 1$ (can be ∞). Thrm: The order of each element in a finite group is finite. Def: Subalgebra $\rho = \langle T, \circ, 1 \rangle$ of group $G = \langle S, \circ, 1 \rangle$ is a subgroup of G if ρ is a group. Thrm: Homomorphic image of a group (monoid, semigroup) is a group (monoid semigroup). THe intersection of two subgroups of a group is a subgroup ($G = \langle S1 \cap S2, \circ, 1 \rangle$).

Boolean Algebra

Def: $\langle S, \oplus, \otimes, \sim, 0, 1 \rangle$ in which:
a) $\oplus$ and $\otimes$ are binary associative operators;
b) $\oplus$ and $\otimes$ are symmetric;
c) 0 and 1 are identities of $\oplus$ and $\otimes$;
d) unary $\sim$ satisfies $b \oplus (\sim b) = 1$ and $b \otimes (\sim b) = 0$.
e) $\otimes$ distributes over $\oplus$: $b \otimes (c \oplus d) = (b \otimes c) \oplus (b \otimes d)$;
f) $\oplus$ distributes over $\otimes$: $b \oplus (c \otimes d) = (b \oplus c) \otimes (b \oplus d)$. Boolean algebra to propositional mapping : $\langle S, \vee, \wedge, \neg, false, true \rangle$ You can use this to prove theorems about boolean algebra from propositional logic.

Idempotency	$b \oplus b = b, b \otimes b = b$
Zero	$b \oplus 1 = 1, b \otimes 0 = 0$
Absorption	$b \oplus (b \otimes c) = b, b \otimes (b \oplus c) = b$
Cancellation	$(b \oplus c = b \oplus d) \wedge (\sim b \oplus c = \sim b \oplus d) \equiv c = d$
	$(b \otimes c = b \otimes d) \wedge (\sim b \otimes c = \sim b \otimes d) \equiv c = d$
Unique complement	$b \oplus c = 1 \wedge b \otimes c = 0 \equiv c = \sim b$
Constant complement	$\sim 0 = 1, \sim 1 = 0$
De Morgan	$\sim (b \oplus c) = (\sim b) \otimes (\sim c), \sim (b \otimes c) = (\sim b) \oplus (\sim c)$
	$b \oplus (\sim c) = 1 \equiv b \oplus c = b, b \otimes (\sim c) = 0 \equiv b \otimes c = b$

Thrm: A homomorphic image of a boolean algebra is a boolean algebra Axiom: $b \leq c \equiv b \otimes c = b$ Theorem. Relation $\leq$ is a partial order. Axiom: $b < c \equiv b \leq c \wedge b \neq c$; $b \leq c \equiv b \oplus c = c$

If an arbitrary boolean algebra $\langle S, \oplus, \otimes, \sim, 0, 1 \rangle$ is isomorphic to a power-set algebra, it must have the equivalent to the empty set and singleton sets. (empty = 0, singletons = atoms)

$atom.a \equiv a \neq 0 \wedge (\forall b : S \mid 0 \leq b \leq a : 0 = b \vee b = a)$
$atom.a \Rightarrow a \otimes b = 0 \vee a \times b = a$ $atom.a \wedge atom.b \wedge a \neq b \Rightarrow a \otimes b = 0$
$(\forall a \mid atom.a : a \otimes b = 0) \Rightarrow b = 0$

Thrm. Any element of finite boolean algebra can be written uniquely as b = y, where y is a "sum" of atoms: $y = (\oplus a \mid atom.a \wedge a \otimes b \neq 0 : a)$ Thrm. A boolean algebra with n atoms has 2^n elements. Thrm. A finite boolean algebra $A = \langle S, \oplus, \otimes, \sim, 0, 1 \rangle$ with n atoms is isomorphic to algebra $\hat{A} = \langle \mathcal{P}\hat{S}, \cup, \cap, \sim, \emptyset, S \rangle$, where $\hat{S} = 1..n$.

Operation Priority

$[x := e]$ (textual substitution) (high precedence)	$**$	$= < > \in \subset \subseteq \supset \supseteq \mid$
	$\cdot / \div$ mod gcd	$\vee \wedge$
	$+ - \cup \cap \times \circ$	$\Rightarrow \Leftarrow$
. (function application)	$\uparrow \downarrow$	$\equiv$ (low precedence)
$+ - \neg \# \sim \mathcal{P}$ (unary prefix operators)	$\#$	
	$\triangleleft \triangleright$ ^	

Definitions

Formal Logic System Let S be a set of interpretations for a logic and F be a formula of the logic.
- F is **satisfiable** (under S) iff at least one interpretation of S maps F to true.
- F is **valid** (under S) iff every interpretation in S maps F to true.
- An **interpretation** is a model for a logic iff every theorem is mapped to true by the interpretation.
- A logic is **sound** iff every theorem is valid.
- A logic is **complete** iff every valid formula is a theorem.
- **Soundness** means that the theorems are true statements about the domain of discourse,
- **Completeness** means that every valid formula can be proved.
- A **sound and complete logic** allows exactly the valid formulas to be proved.
- A boolean expression is **satisfied** in state s iff it evaluates to true in state s.
- A boolean expression is **valid** iff it is satisfied in every state.
- A valid boolean expression is called a **tautology**.
- A boolean expression is **satisfiable** iff there is a state in which it is satisfied.
- The atomic proposition is a type of statement, which contains a truth value that can be true or false.

Sets A set S of sets is a **partition** of a set T if every element of T is exactly one of the elements of S.

Equivalence Relations and Partial Orders An **equivalence relation** must be reflexive, symmetric, and transitive.
A **Partial Order** must be reflexive, anti-symmetric, and transitive.

Final Questions

Properties of set Difference

Question Prove

1. $S - T = S \cap \sim T$	2. $S - T \subseteq S$
3. $S - \emptyset = S$	4. $S \cap (T - S) = \emptyset$
5. $S \cup (T - S) = S \cup T$	6. $S - (T \cup U) = (S - T) \cap (S - U)$
7. $S - (T \cap U) = (S - T) \cup (S - U)$	

Answers
1. $S - T \equiv \{\forall x \mid x \in S \wedge x \notin T\}$ by (11.22), Axiom of Difference. Then $\equiv \{x \mid x \in S \wedge x \in \sim T\}$ by (11.18). Then $\equiv S \cap \sim T$ by (11.21), Axiom of Intersection.
2. Let $x \in S - T$ be arbitrary. Then $x \in S \wedge s \notin T$ by (11.22), Axiom of Difference. Then $x \in S$. Thus by (11.13), Axiom of Subset, $S - T \subseteq S$.
3. $S - \emptyset \equiv \{\forall x \mid x \in S \wedge x \notin \emptyset\}$ by (11.22), Axiom of Difference. Then $\equiv \{x \mid x \in S \wedge x \in \sim \emptyset\}$ by (11.18). Then $\equiv \{x \mid x \in S \wedge x \in U\} \equiv \{x \mid x \in S\} \equiv S$ by (11.17), Axiom of Complement. Thus $S - \emptyset = S$.
4. $S \cap (T - S) \equiv S \cap (T \cap \sim S)$ by (11.49). Then, $\equiv (S \cap \sim S) \cap T \equiv \emptyset \cap T$ by (11.39), Contradiction, and $\equiv \emptyset$, by (11.36), Zero of $\cap$.
5. Since $T - S = T \cap \sim S$, then $S \cup (T - S) \equiv S \cup (T \cap \sim S)$. Consider $s \vee (t \wedge \neg s)$. We have $s \vee (t \wedge \neg s) \equiv (s \vee t) \wedge (s \vee \neg s) \equiv s \vee t$, so the result follows from Methatheorem (11.25).
6. $S - (T \cup U) \equiv S \cap \sim (T \cup U)$ by (11.49). Now consider $s \wedge \neg(t \vee u)$. We have $\equiv s \wedge (\neg t \vee \neg u)$ by De Morgan's Law. Then $\equiv s \wedge \neg t \vee s \wedge \neg u$ by distributivity, so from Methatheorem (11.25), we have $S \cap \sim (T \cup U) \equiv (S \cap \sim T) \cap (S \cap \sim U)$, so from (11.49), we have $S - (T \cup U) \equiv (S - T) \cap (S - U)$.
7. Same thing as (6.).

Assignment 3, Question 11

Question Prove the correctness of the following loop, assigning to F_n the nth fibonacci number:

$$\{Q : n \geq 0\}\ k, b, c := 0, 1, 0;$$
$$\{\text{invariant } P : 0 \leq k \leq n \wedge b = F_{k-1} \wedge c = F_k\}$$
$$\textbf{do } k \neq n \rightarrow k, b, c := k + 1, c, b + c; \textbf{od}$$
$$\{R : c = F_n\}$$

Solution Prove P is $true$ before execution of the loop.

$$P[k, b, c := 0, 1, 0]$$
$$\equiv 0 \leq 0 \leq n \wedge 1 = F_{0-1} \wedge 0 = F_0 \quad \text{(Textual Substitution)}$$
$$\equiv 0 \leq n \wedge 1 = F_{-1} \wedge 0 = F_0 \equiv 0 \leq n$$

Prove P is a loop invariant.

$$P[k, b, c := k + 1, c, b + c]$$
$$\equiv 0 \leq k + 1 \leq n \wedge c = F_{k+1-1} \wedge b + c = F_{k+1} \quad \text{(Textual Substitution)}$$
$$\equiv -1 \leq k \leq n - 1 \wedge c = F_k \wedge b + c = F_{k+1}$$
$$\equiv k \neq n \wedge -1 \leq k \leq n - 1 \wedge c = F_k \wedge b = F_{k+1} - F_k \quad (k \leq n - 1 \Rightarrow k \neq n)$$
$$\Leftarrow k \neq n \wedge 0 \leq k \leq n \wedge c = F_k \wedge b = F_{k+1} - F_k \quad \text{(Strengthening)}$$
$$\equiv k \neq n \wedge 0 \leq k \leq n \wedge c = F_k \wedge b = F_{k-1} \quad \text{(Fibonacci)}$$
$$\equiv P \wedge B \quad \text{(Def. of } P \wedge B\text{)}$$

Prove execution of the loop terminates.
The value of $n - k$ is always at least 0 and it decreases by 1 each iteration; hence, $n - k$ becomes 0 such that the condition is false and the loop terminates.
Prove R holds upon termination.

$$P \wedge \neg B$$
$$\equiv 0 \leq k \leq n \wedge b = F_{k-1} \wedge c = F_k \wedge k = n$$
$$\Rightarrow c = F_k \wedge k = n \quad \text{(Weakening)}$$
$$\equiv c = F_n \quad \text{(Leibniz substitution)}$$

Prove Axiom 9.10 and 9.11

Prove Axiom 9.10 $(\forall x \mid Q \vee R : P) \equiv (\forall x \mid Q : P) \wedge (\forall x \mid R : P)$ by (8.18) Idempotent Range Split. $\Rightarrow (\forall x \mid Q : P)$ by Weakening.
Prove Axiom 9.11 $(\forall x \mid R : P \wedge Q) \equiv (\forall x \mid R : P) \wedge (\forall x \mid R : Q)$ by (8.15), Distributivity. $\Rightarrow (\forall x \mid R : P)$ by Weakening.

Lecture 15, Symmetric Difference

Question Let R be a non-empty binary relation on B. Define the relations R^{ac}, $\prec_1$ and $\prec_2$ on B as follows:
1. $bR^{ac}c \Leftrightarrow bRc \wedge \neg(cR^+b)$ for all $b, c \in B$, i.e. R^{ac} is R after removing all cycles.
2. $b \prec_1 c \Leftrightarrow bR^+c \wedge \neg(cR^+b)$ for all $b, c \in B$, i.e. $\prec_1 = R^+ \cap (\sim R^+) = R^+ \cap (B \times B \setminus R^+)$.
3. $b \prec_2 c \Leftrightarrow bR^{ac}c$

Prove that $\prec_1$ and $\prec_2$ are sharp partial orders and $\prec_2 \subseteq \prec_1$.
Answers Prove 1.: $\prec_1$ is a sharp partial order

- $bR^+b \wedge \neg(bR^+b) \equiv false$ so $\prec_1$ is irreflexive.
- To prove transitivity, consider $b \prec_1 c \prec_1 d \Rightarrow$ $(bR^+c \wedge \neg(cR^+b)) \wedge (cR^+d \wedge \neg(dR^+c)) \Rightarrow bR^+c \wedge cR^+d \equiv c \prec_1 d$.
- To show $\neg(dR^+b)$, assume dR^+b. We already have bR^+c and $dr^+b \wedge bR^+c \Rightarrow dR^+bR^+c \Rightarrow d(R^+ \circ R^+)c \Rightarrow dR^+c$, a contradictoin, as $c \prec_1 d \Rightarrow \neg(dR^+c)$. Thus $\neg(dR^+b)$ must be true.
- Thus $\prec_1$ is transitive, thus it's a sharp partial order.

Prove 2.: $\prec_2$ is a sharp partial order
- $\prec_2$ is transitive because it is a transitive closure of R^{ac}, so only need to prove it is irreflexive.
- $\neg cR^+b$ means that $\neg cR^ib$ for all $i \geq 1$, which means R^{ac} is irreflexive.
- Suppose $b \prec_2 b$ for some $b \in B$. This means $b(R^{ac})^jb$ for some $j \geq 1$. Since R^{ac} is irreflexive, $j > 1$, i.e. $b(R^{ac})^{j-1}cR^{ac}b$. Since R^{ac} is irreflexive, $c \neq b$. But $cR^{ac}b \Rightarrow \neg bR^+c \Rightarrow \forall(i \mid: \neg bR^ic) \Rightarrow \neg bR^{j-1}c \Rightarrow \neg b(R^{ac})^{j-1}c$, a contradiction, $\prec_2$ is irreflexive.
- Thus $\prec_2$ is a sharp partial order.

Prove $\prec_2 \subseteq \prec_1$
- $b \prec_1 c \Leftrightarrow bR^+c \wedge (\neg cR^+b)$ for all $b, c \in B$.
- $b \prec_2 c \Leftrightarrow b(R^{ac})^+c$ where $bR^{ac}c \Leftrightarrow bRc \wedge \neg(cR^+b)$
- We will use the result: if Q is transitive then $Q^+ = Q$ (we will prove it later).
- $bR^{ac}c \Leftrightarrow bRc \wedge \neg(cR^+b) \Leftrightarrow bR^+c \wedge \neg(cR^+b) \Leftrightarrow b \prec_1 c$, so $R^{ac} \subseteq \prec_1$.
- $R^{ac} \subseteq \prec_1 \Rightarrow (R^{ac})^+ \subseteq (\prec_1)^+ = \prec_1$
- Hence $\prec_2 = (R^{ac})^+ \subseteq \prec_1$.

Lecture 15, Prove Binary Relation by Induction

Let R be a transitive relation on B. **Prove** $R^+ = R$.
- Recall $R^+ = \bigcup_{i \geq 1} R^i$, or $bR^+c \equiv \exists(i \mid: i > 0 \wedge bR^ic)$.
- From the definition of R^+, we have $R \subseteq R^+$.
- We now show $R^+ \subseteq R$. By the definition of R^+, it suffices to show $(\forall i \mid 0 < i : R^i \subseteq R)$ by induction.
- Base case: $R \subseteq R$.
- Inductive Step: Assume $R^i \subseteq R$, i.e., $bR^ic \Rightarrow bRc$.
- Consider $bR^{i+1}c \Leftrightarrow \exists(d \mid d \in B : bR^id \wedge dRc) \Leftarrow \exists(d \mid d \in B : bRd \wedge dRc) \Rightarrow bRc$. The last step is by transitivity of R. Hence $R^i \subseteq R$.
- This means $R^+ = R$.

Assignment 3, Question 19

Question Show that $(S, \circ, 1)$ is a group if $\circ$ is a binary associative operator with a left identity 1 and every element has a left inverse.
Answer Prove left cancellation

- We first prove left cancellation, $d \circ b = d \circ c \equiv b = c$.
  - $LHS \Leftarrow RHS$ follows from Leibniz.
  - $LHS \Rightarrow RHS$: $b = d^{-1} \circ d \circ b = d^{-1} \circ d \circ c$ by assumption, so now by identity we have $= c$.
- Prove left idenity is also a right identity: $1 = 1 \equiv 1 \circ 1 = 1 \equiv b^{-1} \circ b \circ 1 = b^{-1} \circ b \equiv b \circ 1 = b$ by left cancelation.
- Since 1 is both left and right identity, it is the unique identity by Theorem (18.2). We now must show that every element has an inverse.
- By assumption, a left inverse exists, so show it is a right inverse.
- Let b^{-1} be the left inverse of b. Then, $b^{-1} = b^{-1} \equiv 1 \circ b^{-1} = b^{-1} \circ 1 \equiv b^{-1} \circ b \circ b^{-1} = b^{-1} \circ 1 \equiv b \circ b^{-1} = 1$.
- Thus we have that there is an inverse.

Prove Boolean Algebra

Question Let $(S, \oplus, \otimes, \sim, 0, 1)$ be a boolean algebra. Prove that for all $b, c, \in S$, we have $b \oplus c = 1 \wedge c \otimes b = 0 \Leftrightarrow c = \sim b$.
- ($\Leftarrow$): from Section Boolean Algebra d), $b \oplus (\sim b) = 1$ and $b \otimes (\sim b) = 0$.
- ($\Rightarrow$): We will start from $c = \sim b$ and work backwards.
- $c = \sim b \Leftrightarrow c \otimes 1 = \sim b \otimes 1 \Leftarrow c \otimes (b \oplus (\sim b)) = \sim b \otimes (b \oplus c) \Leftrightarrow (c \otimes b) \oplus (c \otimes (\sim b)) = 0 \oplus (\sim b \otimes c) \Leftrightarrow c \otimes (\sim b) = (\sim b) \otimes c$ which is true by symmetry.
- Reverse the steps to get the proper proof.

Closures $R^+ = \bigcup_{i=1}^{\infty} aR^ic$ (transitive); $R^* = R^+ \cup i_B$ (reflexive transitive)
18.51 Absorption
$b \oplus (b \otimes c) = (b \otimes 1) \oplus (b \otimes c) = b \otimes (1 \oplus c) = b \otimes 1 < zero >= b$
Cancellation
Prove $b \oplus c = b \oplus d \wedge (\sim b \oplus c = \sim b \oplus d) \equiv c = d$.
- ($\Rightarrow$): $b \oplus c = b \oplus d \wedge (\sim b \oplus c = \sim b \oplus d) <$ Leibniz $c := d >\equiv b \oplus d = b \oplus d \wedge (\sim b \oplus d = \sim b \oplus d) \equiv true \wedge true \equiv true$
- ($\Leftarrow$):
  - $c = d <$ Leibniz $>\equiv b \oplus c = b \oplus d$
  - $c = d <$ Leibniz $>\equiv \sim b \oplus c = \sim b \oplus d$

  Thus $b \oplus c = b \oplus d \wedge (\sim b \oplus c = \sim b \oplus d)$.