MATHEMATICS 300 — SPRING 2006

Introduction to Mathematical Reasoning

H. J. Sussmann—April 17, 2006

1 Some review questions

Review Question 1. Define "equivalence" (of propositional forms). (This is done in the book, p. 5.)

Review Question 2. Define "tautology." (This is done in the book, p. 6.)

Review Question 3. Define "contradiction." (This is done in the book, p. 7.)

Review Question 4. Define "truth set" (of a one-variable predicate). (This is done in the book, p. 20.)

Review Question 5. Define "equivalence" (of one-variable predicates). (This is done in the book, p. 20.)

Review Question 6. Define the predicates "divides" and "is divisible by" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a, b be integers. We say that a **divides** b, or that b **is divisible by** a, if there exists an integer k such that $b = ak$.

IN SYMBOLIC NOTATION: we write "$a|b$" for "a divides b" , or "b is divisible by a", and then "$a|b$" is defined by: $(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(a|b \Leftrightarrow (\exists k \in \mathbb{Z})b = ak)$.

Review Question 7. Define the predicate "is prime" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be an integer. We say that a **is prime** (or a **is a prime number**) if $a > 1$ and there do not exist integers k, ℓ such that $1 < k$, $k < a$, and $a = k\ell$.

IN SYMBOLIC NOTATION:
$(\forall a \in \mathbb{Z})(a$ **is prime** $\Leftrightarrow (a > 1 \wedge \sim (\exists k \in \mathbb{Z})(\exists \ell \in \mathbb{Z})((1 < k \wedge k < a) \wedge a = k\ell)))$.

Review Question 8. Define the predicate "is prime" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the predicate "divides".

ANSWER: Let a be an integer. We say that a **is prime** (or a **is a prime number**) if $a > 1$ and there does not exist an integer k such that $1 < k$, $k < a$, and k divides a.

IN SYMBOLIC NOTATION:
$(\forall a \in \mathbb{Z})(a \textbf{ is prime} \Leftrightarrow (a > 1 \wedge \sim (\exists k \in \mathbb{Z})((1 < k \wedge k < a) \wedge k|a)))$.

Review Question 9. Define the predicate "is even" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be an integer. We say that a **is even** (or a **is an even number**) if there exists an integer k such that $a = k + k$.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is even} \Leftrightarrow (\exists k \in \mathbb{Z})a = k + k)$.

Review Question 10. Define the predicate "is odd" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be an integer. We say that a **is odd** (or a **is an odd number**) if there exists an integer k such that $a = (k + k) + 1$.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is odd} \Leftrightarrow (\exists k \in \mathbb{Z})a = (k + k) + 1)$.

Review Question 11. Define the predicate "is even" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the number 2.

ANSWER: Let a be an integer. We say that a **is even** (or a **is an even number**) if there exists an integer k such that $a = 2k$.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is even} \Leftrightarrow (\exists k \in \mathbb{Z})a = 2k)$.

Review Question 12. Define the predicate "is odd" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the number 2.

ANSWER: Let a be an integer. We say that a **is odd** (or a **is an odd number**) if there exists an integer k such that $a = 2k + 1$.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is odd} \Leftrightarrow (\exists k \in \mathbb{Z})a = 2k + 1)$.

Review Question 13. Define the predicate "is even" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic, the number 2, and the predicate "divides", or "is divisible by".

ANSWER: Let a be an integer. We say that a **is even** (or a **is an even number**) if a is divisible by 2.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is even} \Leftrightarrow 2|a)$.

Review Question 14. Define the predicate "is rational" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be a real number. We say that a **is rational** (or a **is a rational number**) if there exist integers m, n such that n is not equal to zero and $a = \frac{m}{n}$.

IN SYMBOLIC NOTATION:
$(\forall a \in \mathbb{Z})(a \textbf{ is rational} \Leftrightarrow (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})((\sim n = 0) \wedge a = \frac{m}{n}))$.

Review Question 15. Define the predicate "is irrational" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be a real number. We say that a **is irrational** (or a **is an irrational number**) if there do not exist integers m, n such that n is different from zero and $a = \frac{m}{n}$.

IN SYMBOLIC NOTATION:
$(\forall a \in \mathbb{Z})(a \textbf{ is irrational} \Leftrightarrow (\sim (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})((\sim n = 0) \wedge a = \frac{m}{n})))$.

Review Question 16. Define the predicate "is irrational" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the predicate "is rational".

ANSWER: Let a be a real number. We say that a **is irrational** (or a **is an irrational number**) if a is not rational.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is irrational} \Leftrightarrow (\sim a \text{ is rational}))$.

Review Question 17. Define the predicate"is the greatest common divisor of" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the predicate "divides", or "is divisible by".

ANSWER: Let a, b, c be integers. We say that c **is the greatest common divisor of** a **and** b if (i) c divides a, (ii) c divides b, and (iii) if h is any integer such that h divides a and h divides b, it follows that $h \leq c$.

IN SYMBOLIC NOTATION: if we write "GCD" for "greatest common divisor", then

$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(c \textbf{ is the GCD of } a \textbf{ and } b \Leftrightarrow$
$((c|a \wedge c|b) \wedge (\forall h \in \mathbb{Z})((h|a \wedge h|b) \Rightarrow h \leq c)))$.

Review Question 18. Define the predicate"is the greatest common divisor of" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a, b, c be integers. We say that c **is the greatest common divisor of** a **and** b if (i) there exist integers k, ℓ such that $a = kc$ and $b = \ell c$, (ii) if h is any integer such that there exist integers κ, λ for which $a = \kappa h$ and $b = \lambda h$, it follows that $h \leq c$.

IN SYMBOLIC NOTATION: if we write "GCD" for "greatest common divisor", then

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(c \textbf{ is the GCD of } a \textbf{ and } b \Leftrightarrow$$
$$((\exists k \in \mathbb{Z})(\exists \ell \in \mathbb{Z})(a = kc \wedge b = \ell c) \wedge$$
$$(\forall h \in \mathbb{Z})((\exists \kappa \in \mathbb{Z})(\exists \lambda \in \mathbb{Z})(a = \kappa h \wedge b = \lambda h) \Rightarrow h \leq c))) .$$

Review Question 19. Define the predicate"is the least common multiple of" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the predicate "divides", or "is divisible by".

ANSWER: Let a, b, c be integers. We say that c **is the least common multiple of** a **and** b if (i) c is a natural number, (ii) a divides c, (iii) b divides c, and (iv) if h is any natural number such that a divides h and b divides h, it follows that $c \leq h$.

IN SYMBOLIC NOTATION: if we write "LCM" for "least common multiple", then

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(c \textbf{ is the LCM of } a \textbf{ and } b \Leftrightarrow$$
$$((c \in \mathbb{N} \wedge (c|a \wedge c|b)) \wedge (\forall h \in \mathbb{N})((a|h \wedge b|h) \Rightarrow c \leq h))) .$$

Review Question 20. Define "coprime".

ANSWER: Let a, b be integers. We say that a and b are **coprime** if their greatest common divisor is 1.

Review Question 21. Define "absolute value" (of a real number). (The definition is given in the book, page 36.)

Review Question 22. Define "empty set". (This is done in the book, p. 71.)

Review Question 23. Define "subset". (This is done in the book, p. 71.)

Review Question 24. Define "power set". (This is done in the book, p. 74.)

Review Question 25. Define "union" (of two sets). (This is done in the book, p. 78.)

Review Question 26. Define "intersection" (of two sets). (This is done in the book, p. 78.)

Review Question 27. Define "difference" (of two sets). (This is done in the book, p. 78.)

Review Question 28. Define what it means for two sets to be "disjoint". (This is done in the book, p. 79.)

Review Question 29. Define "complement". (This is done in the book, p. 81.)

Review Question 30. Give a recursive (that is, inductive) definition of the "factorial" $n!$ of a natural number n. (This is done in the book, p. 98.)

Review Question 31. Give a recursive (that is, inductive) definition of the "n-th power" a^n, where a is a real number and n is a natural number.

ANSWER: Let a be a real number and let n be a natural number. Then (i) if $n = 1$ then $a^n = a$, (ii) if $n > 1$ then $a^n = a^{n-1} \cdot a$.

IN SYMBOLIC NOTATION:

$(\forall a \in \mathbb{Z})(\forall n \in \mathbb{Z})((n = 1 \Rightarrow a^n = a) \wedge n > 1 \Rightarrow a^n = a^{n-1} \cdot a)$.

Review Question 32. Define "Cartesian product". (This is done in the book, p. 132.)

Review Question 33. Define "relation". (This is done in the book, p. 133.)

Review Question 34. Define "relation from a set A to a set B". (This is done in the book, p. 133.)

Review Question 35. Define "domain" of a relation. (This is done in the book, p. 135.)

Review Question 36. Define "range" of a relation. (This is done in the book, p. 135.)

Review Question 37. Define "inverse" of a relation. (This is done in the book, p. 138.)

Review Question 38. Define "composite" of two relations. (This is done in the book, p. 139.)

Review Question 39. Define "function" from a set A to a set B; you are allowed to use the notions of relation and domain. (This is done in the book, p. 179.)

Review Question 40. Define "function" from a set A to a set B; you are ***not*** allowed to use the notions of relation, domain, or Cartesian product.

ANSWER: Let A, B be sets. A ***function*** from A to B is a set F such that (i) every member of F is an ordered pair (x, y) such that $x \in A$ and $y \in B$, (ii) for every member a of A there exists a $b \in B$ such that $(a, b) \in F$, (iii) whenever $(x, y) \in F$ and $(x, z) \in F$, it follows that $y = z$.

IN SYMBOLIC NOTATION:

$(\forall A)(\forall B)(\forall f)(f$ is a ***function*** $\Leftrightarrow$
$(f$ is a set$\wedge(\forall u)(u \in f \Rightarrow (\exists x)(\exists y)(u = (x, y) \wedge (x \in A \wedge y \in B)))) \wedge$
$(((\forall x)(x \in A \Rightarrow (\exists y)((x, y) \in f \wedge y \in B)) \wedge$
$(\forall x)(\forall y)(\forall z)(((x, y) \in f \wedge (x, z) \in f) \Rightarrow y = z))))$

Review Question 41. Prove that the sum of two even integers is even.

Review Question 42. Prove that the sum of two odd integers is even.

Review Question 43. Prove that the sum of an even integer and an odd integer is odd.

Review Question 44. Prove that if an integer x is odd then $x + 1$ is even. (This is done in the book, p. 32.)

Review Question 45. Prove that if a, b, c are integers, a divides b, and b divides c, then a divides c. (This is done in the book, p. 33.)

Review Question 46. Prove that if a, b, c are integers, a divides b, and a divides c, then a divides $b - c$. (This is done in the book, p. 34.)

Review Question 47. Prove that if a and b are positive integers, and a divides b, then $a \leq b$.

Review Question 48. Prove that if a and b are integers, and a divides b, then $a \leq b$.

Review Question 49. Prove that if n is an odd integer, then either $n = 4j + 1$ for some integer j, or $n = 4i - 1$ for some integer i. (This is done in the book, p. 35.)

Review Question 50. Prove that the sum of two rational numbers is rational.

Review Question 51. Prove that the sum of two irrational numbers is irrational.

Review Question 52. Prove that the sum of a rational number and an irrational numbers is rational.

Review Question 53. Prove that the sum of a rational number and an irrational numbers is irrational.

Review Question 54. Prove that if a and b are positive real numbers, and $a < b$, then $b^2 - a^2 > 0$. (This is done in the book, p. 34.)

Review Question 55. Prove that if a and b are real numbers, and $a < b$, then $b^2 - a^2 > 0$.

Review Question 56. Prove that if x is a real number, then $-|x| \leq x$ and $x \leq |x|$. (This is done in the book, p. 36.)

Review Question 57. Prove that if x and y are real numbers, then $|x+y| \leq |x| + |y|$.

Review Question 58. Prove that every natural number greater than 1 has a prime factor. You may use well-ordering or any form of induction you wish, but I recommend you use well-ordering. (This is done in the book, p. 114.)

Review Question 59. Prove that if p is prime and a, b are positive integers, then p divides the product ab if and only if p divides a or p divides b. (This is done in the book, 42, using the "fundamental theorem of arihtmetic" (FTA). I will acept this proof, even though we did not do the FTA in class. But I am also giving you below a proof that does not use the FTA.)

PROOF (without using the FTA): If p divides a, then we may pick an integer k such that $a = kp$. Then $ab = kbp$, so p divides ab. If p divides b, then we may pick an integer ℓ such that $b = \ell p$. Then $ab = \ell ap$, so p divides ab as well. Therefore, if p divides a or p divides b, then p divides ab. *(Notice that this is a proof by cases.)*

Now assume that p divides ab. We want to prove that p divides a or p divides b. If p divides a, then p divides a or p divides b, so we are done. Next consider the case when p does not divide a. We will prove that p divides b. Since p does not divide a and p is prime, the greatest common divisor of p and a is 1. This implies that we may pick integers m, n such that $ma + np = 1$. Multiplying both sides by b, we get $mab + npb = b$. Since p divides ab, we may pick an integer k such that $ab = kp$. Then $b = mab + npb = mkp + nbp = (mk + nb)p$, so p divides b. **END**

Review Question 60. Prove the set of prime numbers is infinite. More precisely, prove that for every natural numb er N there exists a prime number p such that $p > N$. (This was done in class, and it's done in the book, p. 42.)

PROOF: Let N be a natural number. Let $M = N!$, and let $Q = M + 1$. Then $M+1$ is a natural number and $M+1 > 1$, so $M+1$ has a prime factor p. We will show that $p < N$. Suppose that $p \leq N$. Then $p|N!$. (*Reason: This is intuitively clear, because $N!$ is the product of all the natural numbers from 1 to N, and then p is one of these numbers, since $p \leq N$. Hence $N!$ is a product of natural numbers one of which is p, so $p|N!$. I will accept this argument. But here is a more rigorous proof: we fix p, and show using well-ordering that $(\forall n \in \mathbb{N})(n \geq p \Rightarrow p|n!)$. Call a natural number n "bad" if it is not true that $n \geq p \Rightarrow p|n!$. We want to show that there are no bad numbers. Assume there is one. Then by the well-ordering principle there is a smallest one. Call it b, so b is the smallest bad number. We observe that b cannot be $< p$, because if $b < p$ then the implication "$b \geq p \Rightarrow p|b!$" is true, so b is not bad, and this contradicts the fact that b is bad. So $b \geq p$. Then $b! = (b-1)! \cdot b$, by the inductive definition of the factorial. If $b = p$ then $b! = (b-1)! \cdot p$, so $p|b!$. If $b > p$, then $b - 1$ is a natural number which is not bad, since b is the smallest bad number. So the implication "$b - 1 \geq p \Rightarrow p|(b-1)!$" is true. Since $b - 1 \geq p$, it follows from Rule $\Rightarrow_{use}$ that $p|(b-1)!$. But then $p|(b-1)! \cdot b$, so $p|b!$. We have shown that $p|b!$ in both cases, when $b = p$ and $b > p$. So the implication "$b \geq p \Rightarrow p|b!$" is true in both cases. This shows that b is not bad, and we got a contradiction.*) So $p|M$. Since $p|M + 1$, it follows that $p|1$, which is impossible. So $p > N$. **END**.

Review Question 61. Explain what is wrong with the following "proof": Claim: $-2 = 2$. Proof: Assume that $-2 = 2$. Squaring both sides, we get $4 = 4$, which is true. So our assumption must be true. (This is discussed in the book, p. 58.)

Review Question 62. Prove the *division theorem*: If a, b are integers and $b > 0$ then there exist integers q, r such that $a = bq + r$ and $0 \leq r < b$. (This is done in the notes, p. 101. It is also done in the book, p. 115, under the aditional assumption that $b \leq a$.)

Review Question 63. Prove that if a and b are integers, and a greatest common divisor of a and b exists, then it is unique.

PROOF: We show that, if d and $\tilde{d}$ are two greatest commoon divisors of a and b, then $d = \tilde{d}$. Since $\tilde{d}$ is a GCD of a and b, $\tilde{d}$ is a common divisor of a and b, i.e., $\tilde{d}$ divides a and b. Since d is a GCD of a and b, d is greater than or equal to any common divisor of a and b, so in particular $d \geq \tilde{d}$. A similar argument shows that $\tilde{d} \geq d$. Hence $\tilde{d} = d$. **END**.

Review Question 64. Prove that if a and b are integers, and at least one of them is not zero, then the greatest common divisor d of a and b is an integer linear combination of a and b, that is, there exist integers x, y such that $xa + yb = d$. (This was done in class, and it is also done in the book, p. 115, under the aditional assumption that $a \in \mathbb{N}$ and $b \in \mathbb{N}$.)

Review Question 65. Prove that if r is a rational number then there exist integers m, n such that $n \neq 0$, $r = \frac{m}{n}$, and m, n are coprime.

PROOF: Since r is rational, there exist integers μ, ν such that $\nu \neq 0$ and $r = \frac{\mu}{\nu}$. Let d be the greatest common divisor of μ and ν. Then $d|\mu$, so we may pick $m \in \mathbb{Z}$ such that $\mu = md$. Also, $d|\nu$, so we may pick $n \in \mathbb{Z}$ such that $\nu = nd$. Then $n \neq 0$ (because $\nu \neq 0$ and $\nu = nd$) and $r = \frac{\mu}{\nu} = \frac{md}{nd} = \frac{m}{n}$. Let us show that m and n are coprime. Let g be the greatest common divisor of m and n. Then we may pick $k \in \mathbb{Z}$ amd $\ell \in \mathbb{Z}$ such that $m = kg$ and $n = \ell g$. Then $\mu = kgd$ and $\nu = \ell gd$. So $gd|\mu$ and $gd|\nu$. Therefore $gd \leq d$, since d is the greatest common divisor of μ and ν. Hence $g = 1$, because if $g > 1$ then $gd > d$. So m and n are indeed coprime. **END**.

Review Question 66. Prove that if p is a prime number then $\sqrt{p}$ is irrational.

PROOF: Let $r = \sqrt{p}$. Suppose r is rational. Pick integers m, n such that $r = \frac{m}{n}$ and m and n are coprime. Then $p = r^2 = \frac{m^2}{n^2}$, so $pn^2 = m^2$. It follows that $p|m^2$. Since p is prime and p divides the product $m \cdot m$, it follows that p divides one of the factors, so $p|m$. Pick $k \in \mathbb{Z}$ such that $m = kp$. Then $m^2 = k^2p^2$, so $pn^2 = k^2p^2$, and then $n^2 = k^2p$. Hence $p|n^2$. Since p is prime and p divides the product $n \cdot n$, it follows that p divides one of the factors, so $p|n$. We have thus shown that $p|m$ and $p|n$. So p is a common divisor of m and n. Since m and n are coprime, their greatest common divisor is 1. So $p \leq 1$. But p is prime, so $p > 1$. We have shown that $p \leq 1$ and $p > 1$. This is a contradiction, showing that r is irrational.

Review Question 67. Prove that $\sqrt{15}$ is irrational.

PROOF: Let $r = \sqrt{15}$. Suppose r is rational. Pick integers m, n such that $r = \frac{m}{n}$ and m and n are coprime. Then $15 = r^2 = \frac{m^2}{n^2}$, so $15\,n^2 = m^2$. It follows that $3|m^2$. Since 3 is prime and 3 divides the product $m \cdot m$, it follows that 3 divides one of the factors, so $3|m$. Pick $k \in \mathbb{Z}$ such that $m = 3k$. Then $m^2 = 9k^2$, so $15n^2 = 9k^2$, and then $5n^2 = 3k^2$. Hence $3|5n^2$. Since 3 is prime and 3 divides the product $5 \cdot n \cdot n$, it follows that 3 divides one of the factors, so $3|5$ or $3|n$. Since $\sim 3|5$, we can conclude that $3|n$. We have thus shown that $3|m$ and $3|n$. So 3 is a common divisor of m and n. Since m and n are coprime, their greatest common divisor is 1. So $3 \leq 1$. But $3 > 1$. So $3 \leq 1 \wedge 3 > 1$. This is a contradiction, showing that r is irrational. **END**.

Review Question 68. Is the following proof correct? Explain?

CLAIM: $\sqrt{15}$ is irrational.

PROOF: $\sqrt{15} = \sqrt{3} \cdot \sqrt{5}$. Furthermore, $\sqrt{3}$ is irrational, and $\sqrt{5}$ is irrational. So the product $\sqrt{15}$ is irrational as well. **END**.

Review Question 69. Prove that $\sqrt{18}$ is irrational.