1. Disjunction

Generic Outline of Disjunction:
To prove a disjunction $P \vee Q$:

1. Suppose $\neg P$.
2. Prove Q.

Theorem: For any natural number n, either n is even or n^2 is odd.

Proof: Let n be any natural number. Suppose n is not even. It follows that n is odd. Then there is a natural number k so that $n = 2k + 1$. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

so n is odd. We have proven that if n is any natural number, then either n is even or n^2 is odd. $\square$

2. Cases

Generic Outline of Cases:
To prove cases $(P \vee Q) \rightarrow R$:

1. Prove $P \rightarrow R$
2. Prove $Q \rightarrow R$

Theorem: If a and b are integers, then $|ab| = |a||b|$.

Proof: Let a and b be integers. We will prove that $|ab| = |a||b|$. We will use cases to prove this theorem. The four cases are as follows: $a, b \geq 0$, $a < 0$ and $b \geq 0$, $a \geq 0$ and $b < 0$, or $a, b < 0$.

First, suppose $a, b \geq 0$. This means that

$$|ab| = ab = |a||b|.$$

Thus, $|ab| = |a||b|$.

Next, suppose $a < 0$ and $b \geq 0$. This means that $|a| = -a$ and $|b| = b$. It follows that

$$|(-a)b| = |ab| = (-a)b = |a||b|.$$

Thus, $|ab| = |a||b|$.

Now, suppose $a \geq 0$ and $b < 0$. This means that $|a| = a$ and $|b| = -b$. Then

$$|a(-b)| = |ab| = a(-b) = |a||b|.$$

Thus, $|ab| = |a||b|$.

Finally, suppose $a, b < 0$. Then $|a| = -a$ and $|b| = -b$. That is

$$|(-a)(-b)| = |ab| = (-a)(-b) = |a||b|.$$

Thus, $|ab| = |a||b|$.

Since $|ab| = |a||b|$ for all four cases, we have prove that if a and b are integers, then $|ab| = |a||b|$. □

3. Biconditional

Generic Outline for If-and-only-if: To prove a biconditional $P \leftrightarrow Q$:

1. Prove $P \to Q$
2. Prove $Q \to P$

Theorem: Suppose that d, m, n, q, r are integers so that $m = nq + r$. Then $d|m$ and $d|n$ if and only if $d|n$ and $d|r$.

Proof: Let $d, m, n, q, r \in \mathbb{Z}$ and $m = nq + r$. We will prove $d|m$ and $d|n$ if and only if $d|n$ and $d|r$.

First, suppose $d|m$ and $d|n$. Then there are integers a and b so that $m = da$ and $n = db$. Substituting da in for m and db in for n yields, $dbq + r = da$. Subtracting dbq gives $r = da - dbq$. Then $r = d(a - bq)$. Thus, $d|r$. From our assumption, we also get $d|n$.

Next, suppose $d|n$ and $d|r$. Then there are integers a and b so that $n = db$ and $r = da$. Substituting n and r into the equation for m yields $m = dbq + da$. Factoring out a d gives $m = d(bq + a)$. Thus $d|m$. From our assumption, we also have $d|n$.

We have proven that $d|m$ and $d|n$ if and only if $d|n$ and $d|r$. $\square$

4. Contradiction

Generic Outline for Contradiction: To prove P,

1. Suppose $\neg P$
2. Prove a contradiction
3. Conclude P

Theorem: It is not the case that $2|1$.

Proof: We will prove that it is not the case that $2|1$. We will prove this by way of contradiction.

Suppose $2|1$. By the definition of divisibility, there is an integer k so that $2k = 1$. Then $k + k = 1$. This means $k \leq 1$. There are two cases–either $k = 1$ or $k = 0$. If $k = 0$ then $2 \cdot 0 = 0$. Hence, $1 = 0$ and this is false by Peano Axiom three. If $k = 1$ then $2 \cdot 1 = 2$. Thus, $1 = 2$ and this is false since the successor function is injective and $1 \neq 0$ Then $s(1) \neq s(0)$.

We have proven by way of contradiction that it is not the case that $2|1$. $\square$

5. Contradiction

Generic Outline for Contradiction: To prove P,

1. Suppose $\neg P$
2. Prove a Contradiction
3. Conclude P

Theorem: It is not the case that $0 = 1$.

Proof: We will prove that it is not the case $0 = 1$. We will prove this by way of contradiction.
Suppose $0 = 1$. Then $0 = s(0)$ and this is false by the third Peano Axiom.
Therefore, it is not the case that $0 = 1$. $\square$

6. Subset

Generic Outline for Subset: To prove that a set A is a subset of a set B,

1. Let $a \in A$
2. Prove $b \in B$

Theorem: Suppose that R, S, and T are binary relations on a set A. Then $R \circ (S \circ T) \subseteq (R \circ S) \circ T$.

Proof: Let R, S, and T be binary relations on a set A. We will show that $R \circ (S \circ T) \subseteq (R \circ S) \circ T$.

Suppose $(a, d) \in R \circ (S \circ T)$. This means there is some $b \in A$ with $(a, b) \in R$ and $(b, d) \in S \circ T$. Since $(b, d) \in S \circ T$, there is some $c \in A$ with $(b, c) \in S$ and $(c, d) \in T$. Since $(a, b) \in R$ and $(b, c) \in S$, it follows that $(a, c) \in R \circ S$. Since we also know $(c, d) \in T$, this means $(a, d) \in (R \circ S) \circ T$. Thus, $R \circ (S \circ T) \subseteq (R \circ S) \circ T$. $\square$

7. Set Equality

Generic Outline for Set Equality: To prove a set A equals a set B,

1. Prove $A \subseteq B$
2. Prove $B \subseteq A$

Theorem: Suppose that R is an equivalence relation on a set A and that $a, b \in A$. If aRb, then $[a]_R = [b]_R$.

Proof: Let R be an equivalence relation on a set A and that $(a, b) \in A$. We will prove that if aRb, then $[a]_R = [b]_R$. Suppose aRb. First we will prove $[a]_R \subseteq [b]_R$. Let $x \in [a]_R$. By the definition of equivalence class, aRx. Since R is symmetric, bRa. By transitivity, bRx. Then $x \in [b]_R$. Thus, $[a]_R \subseteq [b]_R$.

Next, we will prove $[b]_R \subseteq [a]_R$. Let $x \in [b]_R$. By the definition of equivalence class, bRx. By transitivity aRx. Then $x \in [a]_R$. Thus, $[b]_R \subseteq [a]_R$.

We have proven that if aRb then $[a]_R = [b]_R$. $\square$

8. Equivalence Relation, Set Equality, Biconditional

Generic Outline for Equivalence Relation: To prove that a binary relation R on a set A is an equivalence relation,

1. Prove that R is reflexive
2. Prove that R is symmetric
3. Prove that R is transitive

Generic Outline for Set Equality: To prove that a set A equals a set B,

1. Prove $A \subseteq B$
2. Prove $B \subseteq A$

Generic Outline for Biconditional: To prove a biconditional $P \leftrightarrow Q$,

1. Prove $P \to Q$
2. Prove $Q \to P$

Theorem: Suppose that R is a reflexive relation on a set A. R is an equivalence relation if and only if $R = R \circ R^{\cup}$.

Proof: Let R be a reflexive relation on a set A. We will prove R is an equivalence relation if and only if $R = R \circ R^{\cup}$.

First, we will prove if R is an equivalence relation then $R = R \circ R^{\cup}$. Suppose R is an equivalence relation. We will prove $R \subseteq R \circ R^{\cup}$. Let $(a, b) \in R$. Then aRb. Since R is reflexive, aRb and bRb. Taking the converse of bRb, yields aRb and $bR^{\cup}b$. Then $aR \circ R^{\cup}b$. Thus, $R \subseteq R \circ R^{\cup}$. Next, we will prove $R \circ R^{\cup} \subseteq R$. Let $(a, c) \in R \circ R^{\cup}$. Then there is a $b \in A$, so that aRb and $bR^{\cup}c$. By the definition of converse, aRb and cRb. Since R is symmetric, aRb and bRc. By transitivity, aRc. Thus, $R \circ R^{\cup} \subseteq R$. Therefore, when R is an equivalence relation, $R \circ R^{\cup} = R$.

Next, we will prove that if $R = R \circ R^{\cup}$ then R is an equivalence relation. Suppose $R = R \circ R^{\cup}$. We will prove that R is an equivalence relation. From our condition above, R is reflexive. We will prove next that R is symmetric. Suppose aRb. Then since R is reflexive, bRb and aRb. By the definition of converse, bRb and $bR^{\cup}a$. It follows that $bR \circ R^{\cup}a$. Thus, bRa and R is symmetric. Next, we will prove that R is transitive. Suppose aRb and bRc. Since we have proven R is symmetric, it follows that aRb and cRb. Applying the converse yields aRb and $bR^{\cup}c$. By the definition of composition, $aR \circ R^{\cup}c$. Thus, aRc and R is transitive. Therefore, when $R = R \circ R^{\cup}$, R is an equivalence relation.

We have proven that R is an equivalence relation if and only if $R = R \circ R^{\cup}$. $\square$

9. Equivalence Relation:

Generic Outline for Equivalence Relation: To prove that a binary relation R on a set A is an equivalence relation,

1. Prove that R is reflexive
2. Prove that R is symmetric
3. Prove that R is transitive

Theorem: Suppose that $f : A \to B$ is any function. Let R be the relation defined on A so if $a, b \in A$, then aRb if and only if $f(a) = f(b)$. R is an equivalence relation.

Proof: Let R be the relation defined on A so that if $a, b \in A$, then aRb if and only if $f(a) = f(b)$. We will prove that R is an equivalence relation.

First, we will prove that R is reflexive. Let $a \in A$. Since $a = a$, $f(a) = f(a)$. Thus, aRa and R is reflexive.

Next, we will prove that R is symmetric. Let $a, b \in A$. Suppose aRb. This means that $f(a) = f(b)$. Since equality is symmetric, $f(b) = f(a)$. Hence, bRa and R is symmetric.

Finally, we will prove that R is transitive. Let $a, b, c \in A$. Suppose aRb and bRc. That is, $f(a) = f(b)$ and $f(b) = f(c)$. Substituting $f(a)$ in for $f(b)$ yields, $f(a) = f(c)$. Therefore, aRc and R is transitive.

We have proven that R is reflexive, symmetric, and transitive. Thus, R is an equivalence relation. $\square$

10. Induction:

Generic Outline for Induction: To prove that $P(n)$ is true for all natural numbers $n \geq m$,

1. Prove $P(m)$
2. Let $k \in \mathbb{N}$ with $m \leq k$
3. Suppose $P(k)$
4. Prove $P(k+1)$

Theorem: For all natural numbers $n \geq 4, n! \geq 2^n$.

*Proof:*Let $P(n)$ be the open statement "$n! \geq 2^n$." We will prove $P(n)$ is true for all natural numbers $n \geq 4$. First, note that $4! = 24 \geq 16 = 2^4$. Thus, $P(4)$ is true.

Next, suppose that k is natural number and that $P(k)$ is true. That is, we are assuming that $k! \geq 2^k$. Observe that, $(k+1)! = (k+1)k!$. Since we assumed $k! \geq 2^k$, it follows that $(k+1)k! \geq (k+1)2^k$. Note that $k+1 \geq 2$. Then $(k+1)k! \geq 2 \cdot 2^k$. Thus, $(k+1)! \geq 2^{k+1}$.

We have proven that $P(4)$ is true and that for all k $P(k)$ implies $P(k+1)$. Thus, by induction $P(n)$ is true for all natural numbers $n \geq 4$. $\square$

11. Induction:

Generic Outline for Induction: To prove that $P(n)$ is true for all natural numbers $n \geq m$,

1. Prove $P(m)$
2. Let $k \in \mathbb{N}$ with $m \leq k$
3. Suppose $P(k)$
4. Prove $P(k+1)$

Theorem: Let s be the sequence defined by $s_0 = 0$ and $s_{n+1} = \dfrac{s_n + 2}{3}$ for all $n \geq 0$. Then s is monotonic.

Proof: Let $P(n)$ be the open statement "$s_n \leq s_{n+1}$." We will use induction to prove that $P(n)$ is true for all natural numbers $n \geq 0$.

First, $s_0 = 0$ and $s_1 = \dfrac{2}{3}$, so $s_0 \leq s_1$ and $P(0)$ is true.

Now suppose that $k \in \mathbb{N}$ and $P(k)$ is true. That is, $s_k \leq s_{k+1}$. Adding 2 to this inequality gives $s_k + 2 \leq s_{k+1} + 2$. Dividing by 3 now gives $\dfrac{s_k + 2}{3} \leq \dfrac{s_{k+1} + 2}{3}$. Our recursive definition of s tells us that $s_{k+1} = \dfrac{s_k + 2}{3}$ and $s_{k+2} = \dfrac{s_{k+1} + 2}{3}$. Hence, we have $s_{k+1} \leq s_{k+2}$. Thus, $P(k+1)$ is true.

We have proven that $P(0)$ is true and that $P(k)$ implies $P(k+1)$ for all natural numbers k. By induction, $P(n)$ is true for all natural numbers $n \geq 0$. It follows that s is increasing. $\square$

12. Induction:

Generic Outline for Induction: To prove that $P(n)$ is true for all natural numbers $n \geq m$,

1. Prove $P(m)$
2. Let $k \in \mathbb{N}$ with $m \leq k$
3. Suppose $P(k)$
4. Prove $P(k+1)$

Theorem: Let s be the sequence defined by $s_1 = 0$ and $s_{n+1} = 1 - s_n$ for all $n \geq 1$. For all n, $s_n = \frac{1}{2}(1 + (-1)^n)$.

Proof: Let s be the sequence defined by $s_1 = 0$ and $s_{n+1} = 1 - s_n$ for all $n \geq 1$. Let $P(n)$ be the open statement "$s_n = \frac{1}{2}(1 + (-1)^n)$." We will prove that $P(n)$ is true for all natural numbers $n \geq 1$. First, note that $s_1 = 0$ and $\frac{1}{2}(1 + (-1)^n) = 0$. Thus, $P(1)$ is true.

Next, suppose that k is a natural number and that $P(k)$ is true. That is, we are assuming that $s_k = \frac{1}{2}(1 + (-1)^k)$. Notice that

$$\begin{aligned} s_{k+1} &= 1 - s_k \\ &= 1 - \frac{1}{2}(1 + (-1)^k) \\ &= 1 - \frac{1}{2} - \frac{1}{2}(-1)^k \\ &= \frac{1}{2} - \frac{1}{2}(-1)^k \\ &= \frac{1}{2}(1 - 1(-1)^k) \\ &= \frac{1}{2}(1 + (-1)^{k+1}). \end{aligned}$$

Hence, $P(k+1)$ is true.

We have established that $P(1)$ is true and that $P(k)$ implies $P(k+1)$. By induction, $P(n)$ is true for all natural numbers $n \geq 1$. $\square$

13. Cardinality:

Generic Outline for Cardinality: To prove that two sets A and B have the same cardinality, exhibit a bijection from A to B.

Theorem: $|\mathbb{Z}| = |\mathbb{N}|$.
Proof: We will prove that $|\mathbb{Z}| = |\mathbb{N}|$. We will define $f : \mathbb{Z} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 2n-1 & n > 0 \\ |2n| & n \leq 0 \end{cases}$$

We will define $g : \mathbb{N} \to \mathbb{Z}$ by

$$g(n) = \begin{cases} \dfrac{n+1}{2} & n\ is\ odd \\ -\dfrac{1}{2}n & n\ is\ even \end{cases}$$

We will prove that f and g are inverses. Let $z \in \mathbb{Z}$. We calculate $g(f(z))$.

$$g(f(z)) = g(2z-1) = \frac{2z-1+1}{2} = \frac{2z}{2} = z.$$

Next let $n \in \mathbb{N}$. We calculate $f(g(n))$.

$$f(g(n)) = f(-\frac{1}{2}n) = |2(-\frac{1}{2}n)| = |-n| = n.$$

Since f and g are inverses, $|\mathbb{Z}| = |\mathbb{N}|$.

$\square$

14. Cardinality:

Generic Outline for Cardinality: To prove that two sets A and B have the same cardinality, exhibit a bijection from A to B.

Theorem: Suppose that A and B are sets. If $|A| = |B|$, then $|\mathcal{P}(A)| = |\mathcal{P}(B)|$.
Proof: Suppose A and B are sets and $|A| = |B|$. We will prove $|\mathcal{P}(A)| = |\mathcal{P}(B)|$. Then there are subsets C and D of A and B, respectively. Define $f : C \to D$ so that

$$F(C) = D = \{f(x) : x \in C\}$$

for $C \subseteq A$. Next, we will define

$$G(D) = \{f^{-1}(x) : x \in D\}$$

for $D \subseteq B$. Since F and G are inverses, f is bijective. There powersets have the same cardinality since A and B have the same cardinality. Thus, $|\mathcal{P}(A)| = |\mathcal{P}(B)|$. $\square$

15. Your Choice: Set Equality

Generic Outline for Set Equality: To prove that a set A equals a set B,

1. Prove $A \subseteq B$
2. Prove $B \subseteq A$

Theorem: Suppose R is an equivalence relation on a set A. Show that $R \circ R = R$.

Proof: Let R be an equivalence relation on a set A. We will prove $R \circ R = R$.

First, we show $R \circ R \subseteq R$. Let $(a, c) \in R \circ R$. This means $aR \circ Rc$. Then there is a $b \in A$ such that aRb and bRc. By transitivity, aRc. Thus, $R \circ R \subseteq R$.

Next, we show $R \subseteq R \circ R$. Let $(a, c) \in R$. This means aRc. By reflexive, aRc and cRc. It follows that $aR \circ Rc$. Thus, $R \subseteq R \circ R$.

Since $R \circ R \subseteq R$ and $R \subseteq R \circ R$, $R \circ R = R$. $\square$