# Discrete Maths Revision Notes

Kevalee Shah

May 19, 2019

## Contents



# 1 Proofs

1. `statement`: a sentence that is either true or false, but not both
2. `predicate`: a statement whose truth relies on the value of one or more variables
3. `contrapositive`: $P \implies Q$ is the same as $\neg Q \implies \neg P$

   Proof strategy: to prove the $P \implies Q$, assume $\neg Q$ and then show that $\neg P$ logically follows
4. $d|n$ means $d$ divides $n$. $n = k \cdot d$ for $d, n, k \in \mathbb{Z}$

   $2|4$ is true but $4|2$ is false

   $d|m \wedge d|n \implies d|m + n$

   $d|m \wedge m|n \implies d|n$
5. $a \equiv b \quad (mod m)$ when $m|(a - b)$

   $18 \equiv -2 \quad (mod 4)$ as $4|20$
6. `universal instantiation` - For an assumption of the form $\forall x.P(x)$, you can strip the quantifier by replacing the $x$ for a variable $c$

   No humans can fly. Bob is human. Therefore Bob cannot fly.

   Humans are $x$ in this case. Bob is $c$

7. Prove: For $n \in \mathbb{Z}$, we have $6|n \quad iff \quad 2|n \wedge 3|n$

   Forward is easy

   Backward: $n = 2 \cdot i$ and $n = 3 \cdot j$. RTP $n = 6 \cdot k$. Let $k = i - j$ ...

8. For every positive integer n, there exists a natural number $l$ such that $2^l \leqslant n < 2^{l+1}$.

9. $l|m \wedge m|n \implies l|n$

10. $\forall n \in \mathbb{Z}, n^2 \equiv 0 \,(mod\, 4) \quad \vee \quad n^2 \equiv 1 \,(mod\, 4)$

11. For prime $p$ and integer $m$ where $0 < m < p$ then $\binom{p}{m} \equiv 0 \quad (mod\, p)$

   Relies on the fact that $\frac{(p-1)!}{m! \cdot (p-m)!}$ is an integer. We know that $\frac{(p)!}{m! \cdot (p-m)!}$ is an integer and that $p|m! \cdot (p-m)!$ is false as $p$ is prime and $m < p$. Therefore $(p-1)!|m!(p-m)!$ must be true, and therefore $\frac{(p-1)!}{m! \cdot (p-m)!} \in \mathbb{Z}$

12. `Binomial Theorem`: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k$ for $n \in \mathbb{N}$

13. $(z+1)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot z^k$ for $n \in \mathbb{N}$

14. $2^n = \sum_{k=0}^{n} \binom{n}{k}$

15. $2^p \equiv 2 \,(modp)$ for prime $p$

16. `Freshman's Dream`: $(m+n)^p \equiv m^p + n^p (modp)$ for natural numbers $m, n$ and prime $p$

   expand the brackets and then use result 11

17. `Dropout Lemma`: $(m+1)^p \equiv m^p + 1 \,(mod\, p)$ for natural numbers $m$ and prime $p$

18. `Many Dropout Lemma`: $(m+i)^p \equiv m^p + i \,(mod\, p)$ for natural numbers $m$ and prime $p$

   $(m+i)^p = ((m+(i-1))+1)^p = (m+(i-1))^p + 1 \,(mod\, p)$

   repeat the above $i$ times

19. `Fermat's little theorem`: $i^p \equiv i \,(mod\, i)$

20. $i^{p-1} \equiv 1 \,(mod\, p)$

21. Logical equivalences

   $\neg(P \implies Q) \iff P \wedge \neg Q$

   $\neg(P \iff Q) \iff P \iff \neg Q$

   $\neg(\forall z. P(x)) \iff \exists x. \neg P(x)$

   $\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$

   $\neg(\exists x. P(x)) \iff \forall x. \neg P(x)$

   $\neg(p \vee Q) \iff (\neg P) \wedge (\neg Q)$

   $\neg(\neg P) \iff P$

   $\neg P \iff P \implies \texttt{False}$

22. $\sqrt{2}$ is irrational

23. $x$ is rational $\iff \exists m, n \in \mathbb{Z}_+$ s.t. $x = \frac{m}{n} \wedge \neg(\exists p : p|m \wedge p|n)$ for prime $p$

    use proof by contradiction

24. $P \implies Q \iff (\neg Q \implies \neg P)$

# 2 Numbers

1. `natural numbers`: counting numbers, including 0

2. `monoid`: set that is closed under an associative binary operation and has identity element $I \in S$ such that $\forall a \in S$, $Ia = aI = a$. Elements do not need to have inverses. The monoid must contain at least one element.

3. `associative monoid`: monoid that is associative

    e.g. $(\mathbb{N}, 0, +)$, $(\mathbb{N}, 1, \cdot)$

4. `group`: monoid with inverses

5. `semiring`: set with two binary operators $S(+, \cdot)$ that satisfies:
    - additive associativity
    - additive commutativity
    - multiplicative associativity
    - left and right distributivity

    e.g. $(\mathbb{N}, 0, +, 1, \cdot)$ is a commutative semiring (with multiplicative commutativity)

6. `ring`: same conditions as a semiring but also has:
    - additive identity
    - additive inverse
    - multiplicative commutativity (for commutative ring)

        e.g. integers $\mathbb{Z}$

7. `field` - set that satisfies the following axioms for both addition and multiplication:
    - associative
    - communtative
    - distributive
    - identity
    - inverse

    e.g. $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$ but not $\mathbb{Z}$

8. `Division Theorem` - For $m \in \mathbb{N}$, $n \in \mathbb{N}_+, \exists\, q, r \in \mathbb{Z}$ such that $q \geqslant 0, 0 \leqslant n < n$ and $m = q \cdot n + r$

9. `Division Algorithm`

```
fun divalg(m, n)
    = let
      fun diviter(q, r)
        = if r < n then (q, r)
          else diviter(q + 1, r - n)
   in
     diviter(0, m)
   end
```

   - This algorithms terminates if `diviter(0, m)` terminates, which terminates if $\exists i \in \mathbb{N}$ such that $m - i \cdot n \leqslant n$, where $i$ is the largest such number. This is always the case and therefore is guaranteed to terminated. ($n$ cannot be 0)
   - In order for the last output to be correct, each intermediate calculation of diviter must also be correct and satisfy: $0 \leqslant q \wedge 0 \leqslant r \wedge m = q \cdot n + r$

     The first call of diviter we have $q = 0, r = m$. $0 \leqslant 0 \ \wedge \ 0 \leqslant m \ \wedge \ m = 0 \cdot n + m$ and therefore satisifies the conditions

     In subsequent calls we have $q = q + 1, r = r - n$. $0 \leqslant q + 1 \wedge 0 \leqslant r - n \ \wedge \ m = (q+1) \cdot n + r - n$ and therefore satisifies the condition

     Therefore when diviter terminates, $q, r$ will be the unique pair of integers that are the quotient and remainder for $m, n$

10. $k \equiv l \, (mod\, m) \iff rem(k, m) = rem(l, m)$ for $m \in \mathbb{Z}_+$ and $k, l \in \mathbb{N}$

11. $n \equiv rem(n, m) \, (mod\, m)$

12. For every integer $k$, there exists unique integer $[k]_m$ such that $0 \leqslant [k]_m < m$ and $k \equiv [k]_m \, (mod\, m)$

    $[k]_m$ = rem(k + $|k| \cdot m$, m)

13. `integers modulo`: $\mathbb{Z}_m$ is the natrual numbers up to $m - 1$

14. `set of divisors`: $D(n) = d \in \mathbb{N} \ : \ d|n$

15. `set of common divisors`: $CD(m, n) = d \in \mathbb{N} \ : \ d|m \wedge d|n$

    $CD(l \cdot n, n) = D(n)$

    $CD(m, n) = CD(n, m)$

16. Let $m, m' \in \mathbb{N}$. Let $n \in \mathbb{Z}_+$ such that $m \equiv m' \, (mod\, n)$. Then we have $CD(m, n) = CD(m', n)$

17. `gcd(m, n)`: Let $x = gcd(m, n)$ Then the following two properties must hold true:

    $x|m \wedge x|n$

For $d \in \mathbb{Z}_+$, $d|m \wedge d|n \implies d|x$

18. `Euclid's Algorithm`

```
fun gcd(m,n) =
  let
    val(q, r) = divalg(m, n)
  in
    if r=0 then n
    else gcd(n, r)
  end
```

Another way to write this is

```
fun gcd(m,n) =
  let
    val q = m div n
    val r = m - nq
  in
    if r=0 then n
    else gcd(n, r)
  end
```

This algorithm is guaranteed to terminate as say we assume that $m > n$. (If it is not the case, in the next step $m, n$ are reversed). Either the algorithm terminates straight away when $n|m$. If not we calculate $gcd(n, r)$. This maintains the ordering and also strictly decreases the second. This process cannot go on forever while maintaining both properties and the fact that the second has to be a positive integer. Therefore algorithm must terminate.

19. $gcd(m, n)|k \cdot m + l \cdot n$ for $k, l \in \mathbb{Z}$

20. If $k \cdot m + l \cdot n = 1$ then $gcd(m, n) = 1$

21. `gcd`: commutative, associative, linear

22. For $k, m, n \in \mathbb{Z}_+$, if $k|m \cdot n$ and $gcd(k, m) = 1$ then $k|n$

23. `Euclid's Theorem`: If $p$ is prime, for $m, n \in \mathbb{Z}_+$ if $p|m \cdot n$ then $p|m$ or $p|n$

    use previous result

24. For prime $p$, every non-zero element $i \in \mathbb{Z}_p$ has $[i^{p-2}]_p$ as inverse. $\mathbb{Z}_p$ is a field.

25. $r \in \mathbb{Z}$ is a linear combination of $m, n \in \mathbb{Z}$ when there exists $s, t \in \mathbb{Z}$ such that $s \cdot m + t \cdot n = r$

26. gcd(m,n) is a linear combination of m and n. To get the linear combination we need to use the `extended euclid's algorithm`

```
fun egcd(m,n) =
  let
    fun egcditer(((s1, t1), r1), lc as ((s2, t2), r2)) =
      let
```

```
            val (q,r) = divalg(r1, r2)
          in
            if r=0 then lc
            else egcditer(lc, ((s1-q*s2), (t1-q*t2), r)
          end
      in
        egcditer(((1,0), m), ((0,1), n))
      end
```

27. $n \cdot lc_1(m, n) \equiv gcd(m, n)\ (mod\, m)$

28. If $gcd(m, n) = 1$ then $[lc_2(m, n)]_m$ is the multiplicative inverse of $[n]_m$ in $\mathbb{Z}_m$

29. `Diffie Hellman Cryptographic Method` - a way to let two people determine a shared key. Two prime numbers $c$ - base (small), $p$ - modulus (big). Alice has own secret number $a$ and sends Bob $A = c^a\ mod\, p$. Bob has his own secret number $b$ and sends Alice $B = c^b\ mod\, p$. Then their shared key is $A^b\ mod\, p = B^a\ mod\, p$

    This relies on the fact that $[([c^a]_p)^b]_p = [([c^b]_p)^a]_p$

30. $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$

    useful to prove binomial theorem

31. `strong induction`: a more general form of mathematical induction

    - Goal: to show $P(n)$ for $n \geqslant a$ ($a$ is the starting point)
    - Basis: prove $P(a), P(a + 1), ..., P(b)$
    - Induction: Assume $P(i)$ for $a \leqslant i \leqslant k$
    - Prove $P(k + 1)$

    useful for proving for $n \geqslant 2, n$ is prime or a product of primes

32. `Fundamental Theorem of Arithmetic`: For every positive integer $n$ there is a unique finite ordered sequence of primes $(p_1 \leqslant \cdots \leqslant p_l,\ l \in \mathbb{N})$ such that $n = \Pi(p_1 \ldots p_l)$

    we can prove uniqueness by saying either $n+1$ is prime or composite. If prime it is unique, else if composite, its the composition of 2 numbers, by strong induction are each unique, and therefore overall it is unique.

33. The set of primes is infinite

    proof by contradiction

# 3 Sets

1. Two sets are equal if they have the same elements

    $\forall$ sets $A, B.A = B \iff (\forall x.x \in A \iff x \in B)$

    $2 = 2, 2$

2. $A \subseteq B \iff \forall x.x \in A \implies x \in B$
3. $A \subset B \iff (\forall x.x \in A \implies x \in B) \wedge A \neq B$
4. `reflexivity`: $A \subseteq A$
5. `transitivity`: $(A \subseteq B \wedge B \subseteq C) \implies A \subseteq C$
6. `antisymmetry`: $(A \subseteq B \wedge B \subseteq A) \implies A = B$
7. Russel's Paradox: $x|x \notin x$ - is this set a member of itself?

    If it is a member of itself then by definition it isnt a member of itself

    If it isn't a member of itself, then it should be a member of itself
8. $x \in A|P(x)$ - prevents Russel's paradox

    $a \in x \in A|P(x) \iff (a \in A \wedge P(a))$
9. $x|x = x$ - universal set
10. $x|x \neq x$ - empty set

    $\varnothing$
11. For any set $A$, the set of all of its subsets is called the power set, denoted $\mathcal{P}(A)$

    $\mathcal{P}(A) = x|x \subseteq A$
12. For all finite sets: $\#\mathcal{P}(A) = 2^{\#A}$
13. $A \cup B = x \in U|x \in A \vee x \in B \in \mathcal{P}(U)$
14. $A \cap B = x \in U|x \in A \wedge x \in B \in \mathcal{P}(U)$
15. $A^c = x \in U|\neg(x \in A) \in \mathcal{P}(U)$
16. Let $U$ be a set, $A, B, C \in \mathcal{P}(U)$ Then:

    $C = A \cup B$ iff

    $A \subseteq C \wedge B \subseteq C$ and

    $\forall X \in \mathcal{P}(U).(A \subseteq X \wedge B \subseteq X) \implies C \subseteq X$
17. Let $U$ be a set, $A, B, C \in \mathcal{P}(U)$ Then:

    $C = A \cap B$ iff

    $C \subseteq A \wedge C \subseteq B$ and

    $\forall X \in \mathcal{P}(U).(X \subseteq A \wedge X \subseteq B) \implies X \subseteq C$
18. $\varnothing \in \varnothing$ but $\varnothing \nsubseteq \varnothing$
19. For every $a$ and $b$ there is a set with $a, b$ as its only elements
20. Product of Sets: $A \times B = x|\exists a \in A \wedge \exists b \in B.x = (a, b)$
21. $\Pi_{i=1}^{n} A = A_1 \times \cdots \times A_n$

    $\Pi_{i=1}^{0} A_i = ()$
22. $\#(A \times B) = \#A \times \#B$

23. Big Union $\bigcup F = x \in U | \exists A \in F. x \in A \in \mathcal{P}(U)$

    $$x \in \bigcup F \iff \exists X \in F. x \in X$$

    $$\bigcup 1, 2, 2, 3 = 1, 2, 3$$

24. Big Intersection $\bigcap F = x \in U | \forall A \in F. x \in A$, for $F \subseteq \mathcal{P}(U)$

    $$\forall x. x \in \bigcap F \iff \forall A \in F, x \in A$$

    $$\bigcap x^n | n \in 0, 1, 2 | x \in 1, 2, 3 = 1$$

25. **Disjoint Union** $A \uplus B = 1 \times A \cup 2 \times B$

26. This means that you can union A and B without losing repeats and being able to identify original set

27. $A \cap B = \varnothing \implies \#(A \cup B) = \#A + \#B = \#(A \uplus B)$

28. Binary Relation: $R : A \mapsto B$

    $R \subseteq A \times B$ or $R \in \mathcal{P}(A \times B)$

    also written as $a\, R\, b$ for $(a, b) \in R$

    Examples:

    - Empty relation: $\varnothing : A \mapsto B$
    - Integer square root $R_2 = (m, n) | m = n^2 : \mathbb{N} \mapsto \mathbb{Z}$

29. Generalised Pigeon Hole Principle: Let $m, n \in \mathbb{Z}_+$. If $m$ objects are put in $n$ boxes and $m > n \cdot k$ for $k \in \mathbb{N}$ then at least one box contains at least $k + 1$ objects.

    For finite sets $A_1 \ldots A_n$, if $\#A_i \leqslant k, \forall 1 \leqslant i \leqslant n$ and $\#(\biguplus_{i=1}^{n} A_i = m)$ then $m \leqslant n \cdot k$

30. Composition of Relations: if $R : A \mapsto B, S : B \mapsto C$ then $S \circ R : A \mapsto C$

    $$a(S \circ R)c \iff \exists b \in B, aRb \wedge bSc$$

31. Directed Graph: $(A, R)$ consists of a set $A$ and a relation $R$ on $A$ (relation from $A$ to $A$)

32. $Rel(A) = \mathcal{P}(A \times A)$ - set of relations on A

33. $(Rel(A), id_A, \circ)$ is a monoid for every set $A$

34. Path of length $n \in \mathbb{N}$ with source $s$ and target $t$, is a tuple $(a_0, \ldots, a_n) \in A^{n+1}$ such that $a_0 = s, a_n = t$ and $a_i R a_i + 1$ for all $0 \leqslant i \leqslant n$

35. $(A, R)$ is a directed graph. For all $n \in \mathbb{N}$ and $s, t \in A, s\, R^{\circ n}\, t$ iif there exsits a path of length $n$ from $s$ to $t$

36. For $R \in Rel(A)$ let $R^{\circ *} = \bigcup R^{\circ n} \in Rel(A) | n \in N = \bigcup_{n \in N} R^{\circ N}$

37. $(A, R)$ is a directed graph. For all $s, t \in A, s\, R^{\circ *} t \iff$ there exists a path with source $s$ and target $t$ in $R$

38. Preorder $(P, \sqsubseteq)$ consists of a set $P$ and a relation $\sqsubseteq$ on $P$ (i.e. $\sqsubseteq \in \mathcal{P}(P \times P)$). It satisfies the following two axioms:

- Reflexivity $\forall x \in P. x \sqsubseteq x$
- Transitivity $\forall x, y, z \in P.(x \sqsubseteq y \wedge y \sqsubseteq z) \implies x \sqsubseteq z$

39. Partial Order (Poset): preorder that further satisfies:

    Antisymmetry $\forall x, y \in P.(x \sqsubseteq y \wedge y \sqsubseteq x) \implies x = y$

40. Partial Function: A relation $R : A \mapsto B$ is said to be functional. It is a partial function when

    $$\forall a \in A. \forall b_1, b_2 \in B. \, a \, R \, b_1 \;\wedge\; a \, R \, b_2 \implies b_1 = b_2$$

    Every a has only one output b

    We write this as $f : A \rightharpoonup B$

    Partial functions do not need to be defined for all their input values

    e.g. if the input and output domains are both $\mathbb{N}$ then $y = \frac{x}{2}$ is not defined for odd numbers.

41. $g(f(a)) = g \circ f$ at $a$
42. $f(a) \downarrow$ indicates that the partial function is defined at $a$
43. For all finite sets $A, B$

    $$\#(A \rightleftharpoons B = (\#B + 1)^{\#A})$$

44. total function: a partial function whose domain of definition coincides with its source.

    $f \; : \; a \rightarrow b$

45. $(A \Rightarrow B) \subseteq (A \rightleftharpoons B) \subseteq Rel(A, B)$
46. For all $f \in Rel(A, B)$,

    $$f \in (A \rightarrow B) \iff \forall \, a \in A. \, \exists! \, b \in B. \, afb$$

47. For all finite sets $A, B$

    $$\#(A \Rightarrow B) = \#B^{\#}A$$

48. Injective: If $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

    Often easier to prove contrapositive: $f(x_1) = f(x_2) \implies x_1 = x_2$

    e.g. $y = x^2$ is not injective.

49. Surjective: For all possible values of $y$, there is some $x$ for which $f(x) = y$
50. Bijective: Must be injective and surjective. A function $f : A \rightarrow B$ is said to be bijective if there exists a function $g : B \rightarrow A$ such that $g$ is a left and right inverse for $f$.
51. $Bij(A, B) \subseteq Fun(A, B) \subseteq PFun(A, B) \subseteq Rel(A, B)$

52. Isomorphic: Two sets are said to be isomorphic and have the same cardinality whenever there is a bijection between them

    $A \cong B$

    $\#A = \#B$

    $\mathbb{N} \cong \mathbb{N}_+$

    $\mathbb{N} \cong \mathbb{Z}$

    $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$

    $\mathbb{N} \cong \mathbb{Q}$

    $\mathbb{N} \ncong \mathbb{R}$

53. partition: A partition, $P$ of set $A$ is a set of non-empty subsets of $A$, that is $P \subseteq \mathcal{P}(A)$ and $\varnothing \notin P$ such that:

    $\bigcup P = A$

    $\forall b_1, b_2 \in P, b_1 \neq b_2 \implies b_1 \cap b_2 = \varnothing$

54. equivalence relation: a binary relation that is reflexive, symmetric and transitive.

    - $\forall x \in A. \, x \, E \, x$
    - $\forall x, y \in A. \, x \, E \, y \implies y \, E \, x$
    - $\forall x, y, z \in A. \, (x : e \to y \wedge y : E \to z) \implies x : E \to z$

    The relation $=$ is the classic example

    Any equivalence relation provides a partition of the underlying set into disjoint equivalence classes

    $$EqRel(A) \cong Part(A)$$

55. For all finite sets $A$

    $$\#EqRel(A) = \#Part(A) = B_{\#A}$$

    where for $n \in \mathbb{N}$ the Bell Numbers are defined by

    $$B_n = \begin{cases} 1 & \text{, for } n = 0 \\ \sum_{i=0}^{m} \binom{m}{i} B_i & \text{, for } n = m + 1 \end{cases}$$

56. Finite Cardinality: A set $A$ is said to be finite whenever $A \cong [n]$ for some $n \in \mathbb{N}$, in which case we write $\#A = n$

57. Infinity Axiom: There is an infinite set, containing $\varnothing$ and closed under successor.

    $$\exists I \, (\varnothing \in I \wedge \forall x \in I((x \cup \{x\}) \in I))$$

    This forms the set of natural numbers

58. $Bij(A, B) \subseteq Sur(A, B) \subseteq Fun(A, B) \subseteq PFun(A, B) \subseteq Rel(A, B)$

59. Enumerability: A set $A$ is said to be enumerable whenever there is a surjection $\mathbb{N} \twoheadrightarrow A$

    a countable set is either empty of enumerable

    $e : \mathbb{N} \twoheadrightarrow A \qquad e(n) \in A | n \in \mathbb{N} = A$

60. Every non-empty subset of an enumerable set is enumerable

61. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countable

62. The product and disjoint unions of countable sets is countable

63. A set $A$ is of less than or equal cardinality to set $B$ whenever there is an injection $A \rightarrowtail B$

    $\#A \leqslant \#B$

    $A \lesssim B$

64. Cantor-Schroeder-Bernstein Theorem: $(A \lesssim B \wedge B \lesssim A) = A \cong B$

65. Cantor's Diagonalisation Theorem: For every set $A$, there is no surjection from $A$ to$\mathcal{P}(A)$

66. Foundation Axiom: The membership relation is well founded

    Infinite chain of $\cdots \in x_n \in \ldots x_1 \in x_0$ not possible

    A set contains no infinitely descending membership sequence

    A set contains a membership minimal element - there is an element of the set that shares no member with the set

$$x \neq \varnothing \implies \exists y \, (y \in x \wedge y \cap x = \varnothing)$$

# 4 Formal Languages and Automata

## 4.1 Regular Expressions

1. Used for representing certain sets of strings in an algebraic way. Satisfy the following rules:
    - Any terminal symbol is in $\Sigma$. This includes the empty and null symbol.
    - Union of two regex is a regex. (e.g. $a|b$)
    - Concat of two regex is a regex (e.g. $ab$)
    - Star of regex is a regex (e.g. $aa$)
    - Regex over $\Sigma$ are precisely those obtained recursively by the application of the above rules once or several times.
2. Identities of Regex
    - $\varnothing + R = R$
    - $\varnothing R + R\varnothing = \varnothing$

- $ER = RE = R$
- $E^* = E$
- $\varnothing^* = E$
- $R|R = R$
- $R^*R^* = R^*$
- $RR^* = R^*R$
- $(R^*)^* = R^*$
- $E|RR^* = E|R^*R = R^*$
- $(PQ)^*P = P(QP)^*$
- $(P|Q)^* = (P^*Q^*)^* = (P^*|Q^*)^*$
- $(P|Q)R = PR|QR$
- $R(P|Q) = RP|RQ$

3. Arden's Theorem: If $P$ and $Q$ are two regex over $\Sigma$, and if $P$ does not contain $\epsilon$ then the following equation in $R$ is given by $R = R|RP$ has a unique solution $R = QP^*$

## 4.2 Pumping Lemma

This is used to prove that a language is **NOT REGULAR**. *It cannot be used to show that a language is regular*

If $A$ is a regular language, then $A$ has a Pumping Length $P$ such that any string $S$ where $|S| \geqslant P$ may be divided into three parts: $S = xyz$ such that the following conditions must be true:

- $xy^iz \in A$ for every $i \geqslant 0$
- $|y| > 0$
- $|xy| \leqslant P$