Graph Coloring

- Let $G = (V, E)$ be an undirected graph.
- A **proper coloring** of $G$ occurs when its nodes are colored so that adjacent nodes have different colors.
- The minimum number of colors needed to color $G$ is the **chromatic number** of $G$ and is written as $\chi(G)$.
- Four colors suffice to color any planar graph.\(^a\)

\(^a\)Appel & Haken (1976). Although the original proof uses a computer, a computer-generated *formal* proof has been given by Gonthier (2004)! This theorem was examined in 1850 by Francis Guthrie (1831–1899) and made its official birth in a letter from DeMorgan to Hamilton in 1852. Kenneth Appel (1932–2013), “Without computers, we would be stuck only proving theorems that have short proofs.”
Graph Coloring (concluded)

- The graph colorability problem for 3 colors and up is computationally hard—it is NP-complete.\(^a\)

- The number of ways to color a graph on \(n\) nodes using \(k\) colors can be calculated in time \(O(2^n n^{O(1)})\).\(^b\)

- \(\chi(G)\) can be calculated in time \(O(2.2461^n)\).\(^c\)

---

\(^a\)Karp (1972).
\(^b\)Bjöklund & Husfeldt (2006).
\(^c\)Bjöklund & Husfeldt (2006).
The four-color theorem says that any map can be colored with just 4 colors.
Elementary Facts

• For all $n \geq 1$, $\chi(K_n) = n$.
  - Each node is adjacent to $n - 1$ other nodes.

• If $H$ is a subgraph of $G$, then $\chi(H) \leq \chi(G)$.
  - A proper coloring of $G$ is also one of $H$.

• An undirected graph $G$ is bipartite if and only if $\chi(G) \leq 2$.
  - Given a bipartite partition $V = V_1 \cup V_2$, color $V_1$ and $V_2$ with two different colors.
An Upper Bound on the Chromatic Number

Theorem 82 (Vizing, 1964; Gupta, 1966)  

Every graph is \((\kappa + 1)\)-colorable, where \(\kappa\) is the maximum degree of the nodes.

1: while \(G(V, E)\) has uncolored nodes do  
2: Pick an arbitrary uncolored \(v \in V\);  
3: Choose color \(c\) that is not used by \(v\)'s \(\leq \kappa\) neighbors;  
4: Color \(v\) with \(c\);  
5: end while
Comments on Vizing’s Theorem

- This bound is tight because $\chi(K_n) = n$ (p. 709).
- Some neighbors may be colored with the same colors if they are not adjacent to each other.
- So $\kappa + 1$ may not be a lower bound for the chromatic number.\(^a\)
- A **clique** is a subgraph that is also a complete graph.
- Is the size of the largest clique in a graph the chromatic number?\(^b\)

\(^a\)Contributed by Mr. Asger K. Pedersen (T02202107) on June 5, 2014.
\(^b\)Contributed by Ms. Zhijing Jin (T05902125) on May 18, 2017.
Coloring 3-Colorable Graphs Efficiently

Theorem 83 (Wigderson, 1983) Any 3-colorable graph can be colored in polynomial time with $O(\sqrt{n})$ colors.

- Surprisingly, no one knows how to do better!\(^a\)

\(^a\)Williamson & Shmoys (2011).
Independent Set

• Let $G = (V, E)$ be an undirected graph.

• An independent set for $G$ is a set of nodes no two of which are adjacent.

• The size of a largest independent set is called the independence number or $\alpha(G)$. 
A Maximum Independent Set
Trees
I love a tree more than a man.
— Ludwig van Beethoven (1770–1827)

Most mathematicians work with calculus-type “smooth” problems, not discrete things like cleverly arranged arrays of zeros and ones.
Trees\textsuperscript{a}

- A **tree** is a loop-free undirected graph that is connected and contains no cycles.

- A **forest** is a loop-free undirected graph whose components are trees.

**Lemma 84** A loop-free connected undirected graph has cycles if and only if it is not a tree.

- By definition of tree.

\textsuperscript{a}Kirchhoff (1847).
A Tree
Spanning Trees

- A **spanning tree** for a connected graph $G = (V, E)$ is a subgraph of $G$ with the same node set $V$ that is also a tree.
  - A (minimum) spanning tree is computationally easy to construct.\(^a\)
  - The number of spanning trees of a connected labeled graph is easy to compute.\(^b\)

- An undirected graph has a spanning tree if and only if it is connected.

\(^a\)Borůvka (1926).
\(^b\)Kirchhoff (1847).
A Spanning Tree

The solid lines constitute the edges of a spanning tree.
Properties of Trees

• If \( x \) and \( y \) are distinct nodes in a tree, then there is a unique path that connects them.
  
  – There is at least one such path because a tree is connected.
  
  – But more than one such path implies the existence of a cycle, a contradiction.
Properties of Trees (continued)

**Theorem 85** For a tree $(V, E)$, $|V| = |E| + 1$.

- Obviously true when $|E| = 0$ as it is a single node.
- In general, a tree with $|E| = k + 1$ edges breaks into two trees $(V_1, E_1)$ and $(V_2, E_2)$ by the deletion of an edge.
- By the induction hypothesis, $|V_1| = |E_1| + 1$ and $|V_2| = |E_2| + 1$.
- Hence,

$$|V| = |V_1| + |V_2| = |E_1| + |E_2| + 2 = |E| + 1.$$
Properties of Trees (continued)

- Theorem 85 (p. 722) may hold for nontrees.
- Consider the following graph:

![Graph Image]

- It satisfies Theorem 85.
- But the graph is not connected.
Properties of Trees (concluded)

The following statements are equivalent for a loop-free undirected graph $G = (V, E)$.

1. $G$ is a tree.

2. $G$ is connected, but the removal of any edge disconnects $G$ into two subgraphs that are trees.


4. $G$ is connected, and $|V| = |E| + 1$.

5. $G$ contains no cycles, and if $x, y \in V$ with $\{x, y\} \not\in E$, then the graph obtained by adding edge $\{x, y\}$ to $G$ has precisely one cycle.
Trees and Forests

**Corollary 86** For a forest \((V, E)\), \(|V| = |E| + \kappa\), where \(\kappa\) is the number of trees in the forest.

- From Theorem 85 (p. 722), \(|V_i| = |E_i| + 1\) for each tree in the forest.
- Hence

\[
|V| = \sum_{i=1}^{\kappa} |V_i| \\
= \sum_{i=1}^{\kappa} (|E_i| + 1) \\
= |E| + \kappa.
\]
Corollary 87  If a loop-free connected undirected graph is not a tree, then $|V| \leq |E|$. 

- Suppose $|V| \geq |E| + 1$ instead.
- Because the graph is not a tree, $|V| > |E| + 1$ by Property 4 on p. 724.
- But then the graph cannot be connected (why?), a contradiction.
Trees Have the Most Nodes among Connected Graphs

**Corollary 88** Among loop-free connected undirected graphs with the same number of edges, trees have the most nodes.

- Consider a graph with $m$ edges.
- From Corollary 87 (p. 726), a nontree must have $\leq m$ nodes.
- But Theorem 85 (p. 722) says that a tree with $m$ edges has $m + 1$ nodes.
Coloring of Trees

**Theorem 89** *Every tree is 2-colorable.*

- Pick any node $v$.
- Color any node reachable from $v$ via an odd number of edges red.
- Color any node reachable from $v$ via an even number of edges blue.
- Because a tree has no cycles,\(^a\) the above operations will not contradict each other at any node.

\(^a\)Recall Lemma 84 (p. 717).
Planarity of Trees

**Lemma 90** *Trees are planar.*

- A tree contains no cycles.
- So it cannot contain a subgraph homeomorphic to either $K_{3,3}$ or $K_5$.
- The lemma follows by Kuratowski’s theorem (p. 697).
Theorem 85 Reproved

• Theorem 85 (p. 722) says $|V| = |E| + 1$ for a tree.

• A tree $(V, E)$ is planar by Lemma 90 (p. 729).

• Then Euler’s theorem (p. 684) says $|V| - |E| + 1 = 2$.

• But this is exactly what Theorem 85 says,

$$|V| = |E| + 1.$$
Legitimate Degree Sequences for Trees

**Theorem 91 (Berge, 1973)** Let $d_1, d_2, \ldots, d_n$ be positive integers. There exists a tree with degrees $d_1, d_2, \ldots, d_n$ if and only if

$$d_1 + d_2 + \cdots + d_n = 2(n - 1).$$

(102)

- A tree on $n$ nodes has $n - 1$ edges by Theorem 85 (p. 722).
- Hence $d_1 + d_2 + \cdots + d_n = 2(n - 1)$ by Eq. (98) on p. 659.
- We next prove the sufficiency of

$$d_1 + d_2 + \cdots + d_n = 2(n - 1)$$

by induction on $n$. 
The Proof (continued)

• As the case \( n \leq 2 \) is trivial, assume \( n \geq 3 \) from now on.

• Assume \( d_1 \leq d_2 \leq \cdots \leq d_n \) without loss of generality.

• \( d_1 = 1 \) because, otherwise,

\[
d_1 + d_2 + \cdots + d_n \geq 2n > 2(n - 1).
\]

• \( d_n > 1 \) because, otherwise,

\[
d_1 + d_2 + \cdots + d_n = n < 2(n - 1).
\]

• Therefore,

\[
d_2 + d_3 + \cdots + (d_n - 1) = 2n - 4 = 2(n - 2).
\]
The Proof (concluded)

- By the induction hypothesis, there exists an \((n-1)\)-node tree \(T\) with degrees \(d_2, d_3, \ldots, d_{n-1}, d_n - 1\).\(^a\)
- Add a new node and join it to the node of \(T\) with degree \(d_n - 1\).
- This \(n\)-node tree has degrees

\[d_1(= 1), d_2, d_3, \ldots, d_n,\]

as desired.

\(^a\)It is not guaranteed that \(d_{n-1} \leq d_n - 1\).
Different Trees May Have the Same Degree Sequence

Contributed by Mr. Jyh-Jau Ma (B91902082) on December 8, 2003.
Remarks

• From Theorem 91 (p. 731), a valid degree sequence $d_1 \leq d_2 \leq \cdots \leq d_n$ of an $n$-node tree must satisfy Eq. (102) on p. 731:

$$d_1 + d_2 + \cdots + d_n = 2n - 2.$$

• We also knew from the proof that $d_1 = 1$ and $d_n > 1$.
  – This fact is a consequence of the above identity.
  – It has nothing to do with whether the graph in question is a tree or not.
Remarks (continued)

- Furthermore, $d_2 = 1$ because, otherwise,\(^a\)
  
  $$d_1 + d_2 + \cdots + d_n \geq 1 + 2(n - 1) = 2n - 1 > 2n - 2.$$  
  
  - Again, this fact is a consequence of 
    $$d_1 + d_2 + \cdots + d_n = 2n - 2$$ alone.
  
  - It has nothing to do with whether the graph in
    question is a tree or not.

- The number of **pendant nodes** (end nodes) in a tree
  with at least 3 nodes is therefore at least 2 and at most
  $n - 1$.

\(^a\)Contributed by Mr. Chun-Hung Hsiao (B91902102), Ms. Microat Wu
(B91902051), and Mr. Jyh-Jau Ma (B91902082) on December 8, 2003.
Remarks (concluded)

- When $n = 3$, then $d_1 = 1, d_2 = 1, d_3 = 2$.
  - As $d_n > 1$ and the tree has 3 nodes, $d_3 = 2$.
  - Finally, $d_2 = 2(n - 1) - d_1 - d_3 = 4 - 1 - 2 = 1$.

- Theorem 91 (p. 731) may hold for nontrees.

- For example, it holds for the following nontree:

  ![Graph Diagram]

- For undirected simple graphs, see Erdős and Gallai (1960).
Degrees, Node Counts, and Edge Counts

**Corollary 92** For a tree $(V, E)$ with degrees $d_1, d_2, \ldots, d_{|V|}$,

\[
|V| = \left( \frac{1}{2} \sum_{i=1}^{\frac{|V|}{2}} d_i \right) + 1,
\]

\[
|E| = \frac{1}{2} \sum_{i=1}^{\frac{|V|}{2}} d_i.
\]

- Theorem 91 (p. 731) says
  \[
d_1 + d_2 + \cdots + d_{|V|} = 2 \times |V| - 2.
  \]
- Theorem 85 (p. 722) says $|V| = |E| + 1$. 

©2018 Prof. Yuh-Dauh Lyuu, National Taiwan University
Number of Valid Degree Sequences

• From Theorem 91 (p. 731), the number of valid degree sequences for $n$-node trees equals the number of integer solutions to

$$d_1 + d_2 + \cdots + d_n = 2(n - 1),$$

where $1 \leq d_1 \leq d_2 \leq \cdots \leq d_n$.

– We must sort them to avoid double counting.

• An equivalent formulation is

$$x_1 + x_2 + \cdots + x_n = n - 2,$$

where $0 \leq x_1 \leq x_2 \leq \cdots \leq x_n$. 
Number of Valid Degree Sequences (continued)

- From p. 532, the desired number equals the coefficient of $x^{n-2}$ in

$$\frac{1}{(1 - x)(1 - x^2) \cdots (1 - x^n)}.$$

  - For instance,

$$\frac{1}{(1 - x)(1 - x^2)(1 - x^3)(1 - x^4)(1 - x^5)} = 1 + x + 2x^2 + 3x^3 + \cdots.$$

  - For 4-node trees, there are 2 valid degree sequences.
  - For 5-node trees, there are 3.
Number of Valid Degree Sequences (concluded)
Number of *Labeled* Trees with Degrees Specified

**Lemma 93** The number of trees with degrees \(d_1, d_2, \ldots, d_n\) on \(n\) labeled nodes \(v_1, v_2, \ldots, v_n\) is

\[
\frac{(n - 2)!}{(d_1 - 1)! (d_2 - 1)! \cdots (d_n - 1)!},
\]

where node \(v_i\) has degree \(d_i > 0, i = 1, 2, \ldots, n\).

- We use induction on \(n\).
- The lemma holds trivially for \(n = 1, 2\).\(^b\)

\(^a\)But counting the number of graphs with a specified degree sequence is hard: It is \#P-complete (Sinclair, 1993).

\(^b\)When \(n = 1\), the formula says \((-1)! / (-1)! = 1\), which is true.
The Proof (continued)

- Without loss of generality, assume $d_n = 1$.\(^a\)
- Now remove node $v_n$, which is adjacent to some node $v_j$.
- The new tree on $\{v_1, v_2, \ldots, v_{n-1}\}$ has degrees

$$d_1, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots, d_{n-1}.$$ 

\(^a\)Recall p. 735.
The Proof (continued)

- By the induction hypothesis, the number of trees with these characteristics is

\[
\frac{(n - 3)!}{(d_1 - 1)! \cdots (d_{j-1} - 1)! (d_j - 2)! (d_{j+1} - 1)! \cdots (d_{n-1} - 1)!} = \frac{(d_j - 1)(n - 3)!}{(d_1 - 1)! \cdots (d_{n-1} - 1)!}.
\]

- By Theorem 91 (p. 731),

\[
\sum_{j=1}^{n-1} (d_j - 1) = \left(\sum_{j=1}^{n-1} d_j\right) - (n - 1) = \left(\sum_{j=1}^{n} d_j\right) - 1 - (n - 1) = 2(n - 1) - n = n - 2.
\]
The Proof (concluded)

• Finally, the number of $n$-node trees with degrees $d_1, d_2, \ldots, d_n$ equals

$$\sum_{j=1}^{n-1} \frac{(d_j - 1)(n - 3)!}{(d_1 - 1)! \cdots (d_{n-1} - 1)!} = \left[ \sum_{j=1}^{n-1} (d_j - 1) \right] \frac{(n - 3)!}{(d_1 - 1)! \cdots (d_{n-1} - 1)!}$$

$$= \frac{(n - 2)(n - 3)!}{(d_1 - 1)! \cdots (d_{n-1} - 1)!} = \frac{(n - 2)!}{(d_1 - 1)! \cdots (d_{n-1} - 1)!}.$$
The Case \((d_1, d_2, \ldots, d_5) = (1, 2, 2, 2, 1)\) with \(n = 5\)

There are \(\frac{3!}{0!0!1!1!1!} = 6\) trees.

\[
\begin{array}{cccccc}
1 & 1 & 1 & 1 & 1 & 1 \\
2 & 2 & 3 & 3 & 4 & 4 \\
3 & 4 & 2 & 4 & 2 & 3 \\
4 & 3 & 4 & 2 & 3 & 2 \\
5 & 5 & 5 & 5 & 5 & 5 \\
\end{array}
\]
$T_n$: The Number of $n$-Node Labeled Trees$^a$

Theorem 94 (Cayley’s formula (1889); Kirchhoff, 1847)

The number of trees on $n$ labeled nodes is

1. $T_n = n^{n-2}$ for $n > 1$,

2. $T_1 = 1$.

• It is trivial to see that $T_1 = 1$.

• Assume $n > 1$ from now on.

$^a$Or, the number of spanning trees of $K_n$ with labeled nodes.
The Proof (continued)

- From Lemma 93 (p. 742) and Eq. (102) on p. 731, the desired number is

\[
\sum_{d_1, \ldots, d_n \geq 1 \atop d_1 + \cdots + d_n = 2n - 2} \frac{(n - 2)!}{(d_1 - 1)! (d_2 - 1)! \cdots (d_n - 1)!}
\]

- We cannot sort the \(d_i\)s because we are dealing with labeled trees.

\[
\sum_{k_1, \ldots, k_n \geq 0 \atop k_1 + \cdots + k_n = n - 2} \frac{(n - 2)!}{k_1! k_2! \cdots k_n!}
\]
The Proof (concluded)

• But

\[ \sum_{k_1,\ldots,k_n \geq 0 \atop k_1+\cdots+k_n=n-2} \frac{(n-2)!}{k_1!k_2!\cdots k_n!} = (1+1+\cdots+1)^{n-2} = n^{n-2} \]

by the multinomial theorem (p. 71).
Arthur Cayley (1821–1895)
The Case $T_4 = 4^2 = 16$
The Case $T_5 = 5^3 = 125$ (p. 741)

There are $5 \times 4 \times 3 = 60$ choices for (a), $\binom{5}{2} \times 3! = 60$ choices for (b), and 5 choices for (c).
Rooted Trees

- Let $G$ be a directed graph.
- $G$ is called a **directed tree** if the undirected graph associated with $G$ is a tree.
- A directed tree $G$ is called a **rooted tree** if there is a unique node $r$, called the root, with an in degree of zero and for all other nodes $v$, the in degree of $v$ is 1.
- A node with an out degree of zero is called a **leaf**.
- Non-leaf nodes are called **internal** nodes.
- The **level number** of a node in a rooted tree is the length of the path from the root to that node.
A Rooted Tree

- The level number of $x$ is 4.
- Don’t ask me why computer scientists plant their trees upside down.
Binary Trees and Beyond

- A rooted tree is called a **binary tree** if the out degree of each node is 0, 1, or 2.
- A rooted tree is called a **complete binary tree** if the out degree of each node is 0 or 2.
- A rooted tree is called an **m-ary tree** if the out degree of each node is at most $m$.
- An $m$-ary tree is called a **complete $m$-ary tree** if the out degree of each node is 0 or $m$. 
A Complete Binary Tree
Properties of Complete \( m \)-Ary Trees

**Theorem 95** For a complete \( m \)-ary tree with \( n \) nodes, \( \ell \) leaves, and \( i \) internal nodes,

1. \( n = mi + 1 \).
2. \( \ell = (m - 1)i + 1 \).
3. \( i = (\ell - 1)/(m - 1) = (n - 1)/m \).

- Need to remove \( m \) leaves to “expose” one internal node.
- Now inductively, \( n - m = m(i - 1) + 1 \), proving property 1.
- Observe that \( \ell = n - i = mi + 1 - i = (m - 1)i + 1 \).
- Property 3 merely restates properties 1 and 2.
A Numerical Example Based on p. 756

• There, $m = 2$, $n = 11$, $\ell = 6$, and $i = 5$.

• We verify the three properties of Theorem 95 below.
  \[ n = mi + 1: \quad 11 = 2 \times 5 + 1. \]
  \[ \ell = (m - 1)i + 1: \quad 6 = (2 - 1) \times 5 + 1. \]
  \[ i = (\ell - 1)/(m - 1) = (n - 1)/m: \]
  \[ 5 = (6 - 1)/(2 - 1) = (11 - 1)/2. \]

• All are satisfied.
Useful Corollaries for Binary Trees

Corollary 96  For a complete binary tree with $\ell$ leaves and $i$ internal nodes,
\[
i = \ell - 1 = (n - 1)/2.\]

- Apply Theorem 95(3) (p. 757) with $m = 2$. 
Useful Corollaries for Binary Trees (concluded)

**Corollary 97** For any binary tree with \(\ell\) leaves and \(i\) internal nodes, \(i \geq (n - 1)/2\) and \(i \geq \ell - 1\).

- For every internal node with an out degree of 1, append a leave node to make its degree 2.
- Suppose \(k \geq 0\) leaves are added in the end.
- As the new tree is a complete binary tree,
  \[
i = \ell + k - 1 = \frac{n + k - 1}{2}
\]
  by Corollary 96.
Additional Properties of Complete Trees

**Theorem 98** Let $T$ be a complete $m$-ary tree with $n$ nodes and $\ell$ leaves. Then

1. $n = (m\ell - 1)/(m - 1)$.
2. $\ell = [(m - 1)n + 1]/m$.

- Let $i$ be the number internal nodes.
- From Theorem 95(1) (p. 757), $n = mi + 1$.
- From Theorem 95(3) (p. 757), $i = (\ell - 1)/(m - 1)$.
- Combine the two to obtain

$$n = m\left[(\ell - 1)/(m - 1)\right] + 1 = (m\ell - 1)/(m - 1).$$
Of Height and Balance

- Let $T$ be a rooted tree.
- If $h$ is the largest level number achieved by a leaf of $T$, then $T$ is said to have **height** $h$.
  - The tree on p. 756 has height 4.
- A rooted tree of height $h$ is said to be **balanced** if the level number of every leaf is $h - 1$ or $h$. 
Height and Number of Leaves

**Theorem 99** Consider a complete $m$-ary tree of height $h$ with $\ell$ leaves. Then

\[ \ell \leq m^h \]

(equivalently, $h \geq \lceil \log_m \ell \rceil$).

- True when $h = 1$ as $T$ is a tree with a root and $\ell = m$ leaves.
- Assume the theorem holds for trees of height less than $h$.
- Consider a tree with height $h$ and $\ell$ leaves.
The Proof (concluded)

- It has $m$ subtrees $T_1, T_2, \ldots, T_m$ at each of the children of the root.

- Let $\ell_i$ be $T_i$’s number of leaves and $h_i \leq h - 1$ be $T_i$’s height.

- $\ell_i \leq m^{h_i} \leq m^{h-1}$ by the induction hypothesis.

- So

$$\ell = \ell_1 + \ell_2 + \cdots + \ell_m \leq m(m^{h-1}) = m^h.$$
Height and Number of Leaves of Balanced Trees

**Corollary 100** Consider a balanced complete \( m \)-ary tree with \( \ell \) leaves. Then its height \( h \) equals \( \lceil \log_m \ell \rceil \).

- \( \ell \leq m^h \) by Theorem 99 (p. 763).
- \( m^{h-1} < \ell \) because there are already \( m^{h-1} \) nodes with a level number of \( h - 1 \) (prove it!).

Hence

\[ \lceil \log_m \ell \rceil \leq h < \log_m \ell + 1 \leq \lceil \log_m \ell \rceil + 1. \]

- As \( h \) must be an integer, \( h = \lceil \log_m \ell \rceil \).
Rings and Modular Arithmetic
It you tackle a problem and seem to get stuck,
Just take it mod $p$ and you’ll have better luck.

— Tom M. Apostol (1955)
and Saunders MacLane (1973),

*Where Are the Zeros of Zeta of $s$?*
Rings\textsuperscript{a}

• Let $R$ be a nonempty set endowed with 2 \textit{closed} binary operations “$+$” and “$\cdot$”.

• $(R, +, \cdot)$ is a \textbf{ring} if the following conditions hold for all $a, b, c \in R$.
  
  \begin{itemize}
    
    \item $a + b = b + a$ (commutative law of $+$).
    
    \item $a + (b + c) = (a + b) + c$ (associative law of $+$).
    
    \item There exists $z \in R$ such that $a + z = z + a = a$ for every $a \in R$ (existence of the \textbf{additive identity} or \textbf{zero element} for $+$).
  \end{itemize}

\textsuperscript{a}Named by David Hilbert (1862–1943).
Rings (concluded)

• (continued)
  – For each \( a \in R \), there is a \( b \in R \) with
    \[ a + b = b + a = z \] (existence of additive inverse).
  – \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \) (associative law of \( \cdot \)).
  – \( a \cdot (b + c) = a \cdot b + a \cdot c \) and \( (b + c) \cdot a = b \cdot a + c \cdot a \) for
    all \( a, b, c \in R \) (distributive laws of \( \cdot \) over +).

• In additional, the ring is said to be **commutative** if
  \[ a \cdot b = b \cdot a \]
  for all \( a, b, \in R \).
David Hilbert (1862–1943)
Comments

• It is helpful but dangerous to think of “+” as addition and “·” as multiplication.

• From the definitions,
  – A ring has an additive identity $z$ (sometimes 0).
  – The additive inverse exists in a ring.

• A $u \in R$ is called a multiplicative identity or unity if $u \neq z$ and $a \cdot u = u \cdot a = a$ for all $a \in R$.
  – Sometimes, $u$ is denoted by 1.

• The multiplicative identity may not exist in a ring.
Comments (concluded)

• If a ring contains a multiplicative identity, then it is called a ring with unity.

• An element $b \in R$ is said to be $a$’s multiplicative inverse if

$$a \cdot b = b \cdot a = 1.$$ 

• A multiplicative inverse is not guaranteed to exist in a ring.

• If $a \in R$ has a multiplicative inverse, $a$ is called a unit.
Some Basic Facts

• \((\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)\) are all rings.
  
  − The additive identity is 0.
  
  − The additive inverse of each number \(x\) is written as \(-x\).\(^a\)

• In any ring, the zero element \(z\) (i.e., the additive identity) is unique.
  
  − If \(z_1\) and \(z_2\) are additive identities, then

\[
\begin{align*}
z_1 &= z_1 + z_2 = z_2.
\end{align*}
\]

\(^a\)Note that “−” is not in the language of rings; it is merely a shorthand for the additive inverse.
Some Basic Facts (concluded)

- The additive inverse of a ring element is also unique.
  - For \( a \in R \), suppose there are elements \( b, c \in R \) where
    \[
    a + b = b + a = z,
    \]
    \[
    a + c = c + a = z.
    \]
  - Then
    \[
    b = b + z = b + (a + c) = (b + a) + c = z + c = c.
    \]
A Useful Shorthand

- Let $(R, +, \cdot)$ be a ring.
- Consider $kx$, where $k \in \mathbb{Z}^+$ and $x \in R$.
- This is clearly not an operation in $R$ because $k \notin R$.
- In fact, it is merely a shorthand for $\underbrace{k}_{x + \cdots + x}$. 
Rings with Sets

• Let $U$ be a finite set.

• Consider $(R, +, \cdot) = (2^U, \Delta, \cap)$.
  - $A + B = A \Delta B$ for $A, B \subseteq U$.\(^a\)
  - $A \cdot B = A \cap B$ for $A, B \subseteq U$.

• It is not hard to see that $(2^U, \Delta, \cap)$ is a ring with unity.

• The additive identity is $\emptyset$.

• The multiplicative identity is $U$.

• This example shows it is dangerous to think of “$+$” as addition and “$\cdot$” as multiplication exclusively.

\(^a\)Recall Eq. (25) on p. 194 for the symmetric difference.
Generalized Distributive Laws

**Lemma 101** Let \((R, +, \cdot)\) be a ring. Then

\[(a_1 + \cdots + a_m) \cdot (b_1 + \cdots + b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i \cdot b_j\]

for \(m, n \in \mathbb{Z}^+\) and \(x, y \in R\).\(^a\)

Proof: By induction, it equals

\[(a_1 + \cdots + a_m) \cdot b_1 + \cdots + (a_1 + \cdots + a_m) \cdot b_n = a_1 \cdot b_1 + a_2 \cdot b_1 + \cdots + a_m \cdot b_n.\]

\(^a\)Again, \(\sum\) is a shorthand.
A Practice Run

**Lemma 102** Let $(R, +, \cdot)$ be a ring. Then

$$(kx) \cdot (jy) = (kj)(x \cdot y) \text{ for } k, j \in \mathbb{Z}^+ \text{ and } x, y \in R.$$  

Proof:

\[
(kx) \cdot (jy) = \overbrace{(x + \cdots + x)}^{k} \cdot \overbrace{(y + \cdots + y)}^{j} = \underbrace{x \cdot y + \cdots + x \cdot y}_{kj} = (kj)(x \cdot y),
\]

where the second equality is by Lemma 101 (p. 777).
Lemma 103  Let \((R, +, \cdot)\) be a ring. Then
\((kx) \cdot (jy) = ((kj)x) \cdot y\) for \(k, j \in \mathbb{Z}^+\) and \(x, y \in R\).

Proof:
\[
(kx) \cdot (jy) = \underbrace{x + \cdots + x}_{k} \cdot \underbrace{y + \cdots + y}_{j}
\]
\[
= \underbrace{x \cdot y + \cdots + x \cdot y}_{kj}
\]
\[
= \underbrace{(x + \cdots + x)}_{kj} \cdot y
\]
\[
= ((kj)x) \cdot y,
\]
where the third equality is by Lemma 101 (p. 777).
The Cancellation Laws of +

**Theorem 104**  For all \( a, b, c \in R \), (a) \( a + b = a + c \) implies \( b = c \), and (b) \( b + a = c + a \) implies \( b = c \).

- We focus on (a).
- As \( a \in R \), it follows that \( -a \in R \).
- Hence
  \[
  a + b = a + c \quad \Rightarrow \quad (-a) + (a + b) = (-a) + (a + c) \\
  \Rightarrow \quad [( -a ) + a] + b = [( -a ) + a] + c \\
  \Rightarrow \quad z + b = z + c \\
  \Rightarrow \quad b = c.
  \]
Comments

• In the proof, we implicitly used the following property:

   \[ \text{if } b = c, \text{ then } a + b = a + c. \]

• This is the opposite of the cancellation law.

• It is true because the left and right sides are identical.
A Corollary

Corollary 105  For any ring \((R, +, \cdot)\) and any \(a \in R\),

\[ a \cdot z = z \cdot a = z. \]

- \(a \cdot z + a \cdot z = a \cdot (z + z) = a \cdot z.\)
- By the left-cancellation property (p. 780), \(a \cdot z = z.\)
A Criterion for Commutativity

**Lemma 106** Let \((R, +, \cdot)\) be a ring. It is commutative if and only if \((a + b)^2 = a^2 + 2(a \cdot b) + b^2\) for all \(a, b \in R\).

- Note that
  \[(a + b)^2 = (a + b) \cdot (a + b) = a^2 + b \cdot a + a \cdot b + b^2.\]

- So if \((a + b)^2 = a^2 + 2(a \cdot b) + b^2\), then
  \[2(a \cdot b) = a \cdot b + b \cdot a.\]

- As \(2(a \cdot b) = a \cdot b + a \cdot b\), the above and the left-cancellation property (p. 780) imply \(a \cdot b = b \cdot a\).

- The other direction is trivial.