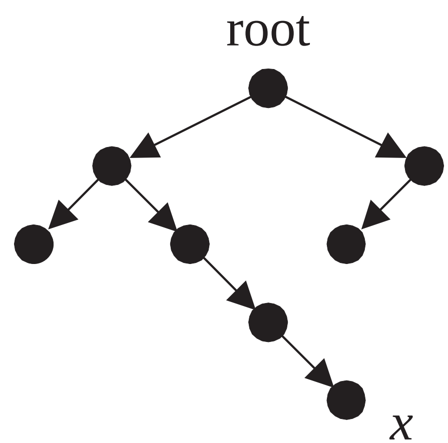
Rooted Trees

- Let G be a directed graph.
- G is a **directed tree** if its undirected version is a tree.
- A directed tree G is called a **rooted tree** if (1) there is a unique node r, called the root, with an in degree of zero and (2) 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

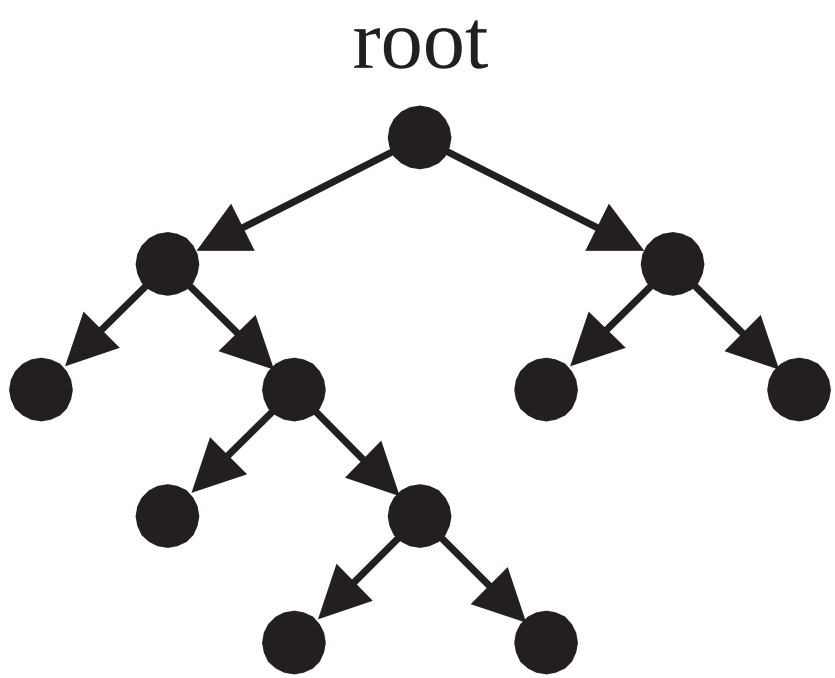


- The level number of x is 4.
- Don't ask me why computer scientists plant their trees upside down.

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 89 *For a complete m-ary tree with n nodes, ℓ leaves, and i internal nodes,*

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

- 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. 738

- There, $m = 2$, $n = 11$, $\ell = 6$, and $i = 5$.
- We verify the three properties of Theorem 89 below.

  $\boldsymbol{n = mi + 1}$**:** $11 = 2 \times 5 + 1$.

  $\boldsymbol{\ell = (m-1)i + 1}$**:** $6 = (2-1) \times 5 + 1$.

  $\boldsymbol{i = (\ell - 1)/(m-1) = (n-1)/m}$**:**
  $$5 = (6-1)/(2-1) = (11-1)/2.$$
- All are satisfied.

Useful Corollaries for Binary Trees

Corollary 90 *For a complete binary tree with ℓ leaves and i internal nodes,*

$$i = \ell - 1 = (n-1)/2.$$

- Apply Theorem 89(3) (p. 739) with $m = 2$.

Useful Corollaries for Binary Trees (concluded)

Corollary 91 *For any binary tree with ℓ 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 with $\ell + k$ leaves,
$$i = (\ell + k) - 1 = \frac{(n+k)-1}{2}$$
by Corollary 90.

Additional Properties of Complete Trees

Theorem 92 *Let T be a complete m-ary tree with n nodes and ℓ leaves. Then*

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

- Let i be the number internal nodes.
- By Theorem 89(1) (p. 739), $n = mi + 1$.
- By Theorem 89(3) (p. 739), $i = (\ell - 1)/(m - 1)$.
- Combine the two to obtain

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

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. 738 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 93 *Consider a complete m-ary tree of height h with ℓ 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 ℓ leaves.

The Proof (concluded)

- It has m subtrees $T_1, T_2, \ldots, T_m$ at each of the children of the root.
- Let ℓ_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
$$\ell = \ell_1 + \ell_2 + \cdots + \ell_m \leq m\left(m^{h-1}\right) = m^h.$$

Height and Number of Leaves of Balanced Trees

Corollary 94 *Consider a balanced complete m-ary tree with ℓ leaves. Then its height h equals $\lceil \log_m \ell \rceil$.*

- $\ell \leq m^h$ by Theorem 93 (p. 745).
- $m^{h-1} < \ell$ 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[a]

- Let R be a nonempty set endowed with 2 *closed* binary operations "$+$" and "$\cdot$".
- $(R, +, \cdot)$ is a **ring** if the following conditions hold for all $a, b, c \in R$.
  - $a + b = b + a$ (commutative law of $+$).
  - $a + (b + c) = (a + b) + c$ (associative law of $+$).
  - There exists $z \in R$ such that $a + z = z + a = a$ for every $a \in R$ (existence of the **additive identity** or **zero element** for $+$).

[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 addition, 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 to think of "+" as addition and "·" as multiplication.
- From the definitions,
  - A ring has an *additive* identity z (sometimes 0).
  - The *additive* inverse always exists in a ring.
- A $u \in R$ is called a **multiplicative identity** or simply **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.
- If $a \in R$ has a multiplicative inverse, it is called a **unit**.

Some Basic Facts

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are rings.
  - The additive identity is 0.
  - The additive inverse of each number x is written as $-x$.[a]
- For any ring, the zero element z (i.e., the additive identity) is unique.
  - If z_1 and z_2 are additive identities, then

$$z_1 = z_1 + z_2 = z_2.$$

[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

$$\begin{aligned} a + \boxed{b} &= \boxed{b} + a = z, \\ a + \boxed{c} &= \boxed{c} + a = z. \end{aligned}$$

  - Then

$$b = b + z = b + (a + c) = (b + a) + c = z + c = c.$$

Useful Shorthands

- Let $(R, +, \cdot)$ be a ring.
- Consider ka, where $k \in \mathbb{Z}^+$ and $a \in R$.
- This is clearly *not* an operation in R because $k \notin R$.
- Instead, it is a shorthand for

$$((\overbrace{(a + a) + a) + \cdots) + a}^{k} = \overbrace{a + \cdots + a}^{k}.$$

- We write $a_1 + a_2 + \cdots + a_k$ or $\sum_{i=1}^{k} a_i$ instead of $((a_1 + a_2) + \cdots) + a_k$ by the associative law of $+$.

Useful Shorthands (concluded)

- Similarly, we write a^k for

$$\overbrace{a \cdot a \cdot \cdots \cdot a}^{k},$$

  where $k > 0$.

- We write $a_1 \cdot a_2 \cdot \cdots \cdot a_k$ or $\prod_{i=1}^{k} a_i$ instead of $((a_1 \cdot a_2) \cdot \cdots) \cdot a_k$ by the associative law of $\cdot$.

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.
- So it is incorrect to think of "+" as addition and "·" as multiplication exclusively.

---

[a] Recall Eq. (26) on p. 197 for the symmetric difference.

Generalized Distributive Laws

Lemma 95 *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* $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n \in R$.

Proof: By induction, it equals

$$\begin{aligned} & (a_1 + \cdots + a_m) \cdot b_1 + \cdots + (a_1 + \cdots + a_m) \cdot b_n \\ = \; & a_1 \cdot b_1 + a_2 \cdot b_1 + \cdots + a_m \cdot b_n. \end{aligned}$$

A Practice Run

Lemma 96 *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:

$$
\begin{aligned}
(kx) \cdot (jy) &= (\overbrace{x + \cdots + x}^{k}) \cdot (\overbrace{y + \cdots + y}^{j}) \\
&= \overbrace{x \cdot y + \cdots + x \cdot y}^{kj} \\
&= (kj)(x \cdot y),
\end{aligned}
$$

where the second equality is by Lemma 95 (p. 760).

Another Practice Run

Lemma 97 *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:

$$\begin{aligned}
(kx) \cdot (jy) &= (\overbrace{x + \cdots + x}^{k}) \cdot (\overbrace{y + \cdots + y}^{j}) \\
&= \overbrace{x \cdot y + \cdots + x \cdot y}^{kj} \\
&= (\overbrace{x + \cdots + x}^{kj}) \cdot y \\
&= ((kj)x) \cdot y,
\end{aligned}$$

where the third equality is by Lemma 95 (p. 760).

The Cancellation Laws of $+$

Theorem 98 *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

$$
\begin{aligned}
a+b=a+c \quad & \Rightarrow \quad (-a)+(a+b)=(-a)+(a+c) \\
& \Rightarrow \quad [\,(-a)+a\,]+b=[\,(-a)+a\,]+c \\
& \Rightarrow \quad z+b=z+c \\
& \Rightarrow \quad b=c.
\end{aligned}
$$

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 99 *For any ring* $(R, +, \cdot)$ *and any* $a \in R$,

$$a \cdot z = z \cdot a = z.$$

- $a \cdot z + a \cdot z = a \cdot (z + z) = a \cdot z = a \cdot z + z.$
- By the left-cancellation property,[a]

$$a \cdot z = z.$$

---

[a]Recall p. 763.

A Criterion for Commutativity[a]

Lemma 100 *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
$$(a+b)^2 = (a+b) \cdot (a+b) = a^2 + \boxed{a \cdot b + b \cdot a} + b^2.$$
- 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 imply $a \cdot b = b \cdot a$.
- The other direction is trivial.

[a] Recall p. 751.

Additional Properties

Corollary 101 *For any ring* $(R, +, \cdot)$, *for all* $a, b \in R$,

1. $-(-a) = a$.
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.
3. $(-a) \cdot (-b) = a \cdot b$.

- By definition $-(-a)$ is the additive inverse of $-a$.
- As $(-a) + a = z$, a is also the additive inverse of $-a$.
- By the uniqueness of the additive inverse,[a] $-(-a) = a$, establishing (1).

---

[a]Recall p. 755.

The Proof (concluded)

- By definition $-(a \cdot b)$ is *the* additive inverse of $a \cdot b$.
- But by Corollary 99 (p. 765),

$$a \cdot b + \boxed{a \cdot (-b)} = a \cdot [\, b + (-b)\,] = a \cdot z = z.$$

- By the uniqueness of the additive inverse,[a]
  $a \cdot (-b) = -(a \cdot b)$.
- Similarly, $(-a) \cdot b = -(a \cdot b)$, establishing (2).
- From (2), $(-a) \cdot (-b) = -[\, a \cdot (-b)\,] = -[\, -(a \cdot b)\,]$.
- Part (3) follows from (1).

[a] Recall p. 755 again.

The Uniqueness of Unity[a]

Theorem 102 *Let* $(R, +, \cdot)$ *be a ring with unity.*[b] *(a) The unity is unique. (b) If* x *is a unit of* R*, then the multiplicative inverse of* x *is unique.*

- As a result, u (or 1) is *the* unity of a ring with unity.
- Furthermore, the multiplicative inverse of each unit x will be denoted by x^{-1}.

---

[a] Prove it!

[b] Recall p. 753.

Proper Divisor of Zero

- A ring may contain **proper divisors of zero**.
- a is a proper divisor of zero if $a \neq z$ and there exists a $b \neq z$ such that $a \cdot b = z$ or $b \cdot a = z$.
  - The set of 2×2 integral matrices with matrix addition and multiplication is a ring.[a]
  - But

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

[a]It is not commutative, however.

Units Are Not Proper Divisors of Zero

Lemma 103 *A unit in a ring R cannot be a proper divisor of zero.*

- Let $x \in R$ be a unit.[a]
- So there exists a $y \in R$ such that $x \cdot y = y \cdot x = 1$.
- Suppose $x \cdot w = z$ for some $w \in R$.
- By Corollary 99 (p. 765),
$$y \cdot (x \cdot w) = y \cdot z = z.$$
- But
$$y \cdot (x \cdot w) = (y \cdot x) \cdot w = 1 \cdot w = w.$$
- Hence $w = z$, and x is not a proper divisor of zero.

[a] Recall p. 754.

Integral Domains and Fields[a]

- Let $(R, +, \cdot)$ be a commutative ring with unity.
- R is called an **integral domain** if R has no proper divisors of zero.
- R is called a **field** if every nonzero element is a unit.

[a]Due to Evariste Galois.

Evariste Galois (1811–1832)

Some Examples

- $(\mathbb{Z}, +, \cdot)$ is an integral domain but not a field.
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are integral domains and fields.

Fields Are Integral Domains

Theorem 104 *If* $(F, +, \cdot)$ *is a field, then it is an integral domain.*

- Let $a, b \in F$ with $a \cdot b = z$.
- If $a = z$, then we are done.
- So assume $a \neq z$.
- Then a has a multiplicative inverse a^{-1} as F is a field.
- Now, $a \cdot b = z$ implies

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot z = z$$

by Corollary 99 (p. 765).

The Proof (concluded)

- But
$$a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = u \cdot b = b.$$
- Hence $b = z$.
- We conclude that F has no proper divisors of zero.

Finite Integral Domains Are Fields

Theorem 105 *A finite integral domain* $(D, +, \cdot)$ *is a field.*

- Assume $D = \{ d_1, d_2, \ldots, d_n \}$.
- For $d \in D$ such that $d \neq z$,

$$dD \triangleq \{ d \cdot d_1, d \cdot d_2, \ldots, d \cdot d_n \} \subseteq D$$

  because D is closed under $\cdot$.
- Suppose $| dD | < n$.
- Then

$$d \cdot d_i = d \cdot d_j$$

  for some distinct i, j.

The Proof (concluded)

- As D is an integral domain and $d \neq z$, it follows that

$$d_i = d_j$$

  by the cancellation law, a contradiction.

- We conclude that $|\, dD \,| = n$ and thus $dD = D$.
- As a result, $d \cdot d_k = u$, the unity of D, for some $1 \leq k \leq n$.
- This implies d is a unit of D.
- Because this is true for all $d \neq z$, $(D, +, \cdot)$ is a field.

The Integers Modulo n

- Let $n \in \mathbb{Z}^+$, $n > 1$.
- For $a, b \in \mathbb{Z}$, we say a is **congruent**[a] **to** b **modulo** n, written $a \equiv b \bmod n$, if $n \mid (a - b)$.[b]
- n is the **modulus**.
- Congruence modulo n is an equivalence relation on $\mathbb{Z}$.[c]
- Let $\mathbb{Z}_n$ be the equivalence classes:

$$\mathbb{Z}_n = \{\, 0, 1, \ldots, n-1 \,\}.$$

  – $\mathbb{Z}_n = \{\, [\,0\,], [\,1\,], \ldots, [\,n-1\,] \,\}$ is more precise.

---

[a] Carl Friedrich Gauss.

[b] Or a and b are **congruent modulo** n.

[c] Recall p. 395.

Carl Friedrich Gauss (1777–1855)

$a \equiv b \bmod n$ vs. $a = b \bmod n$

- $a \equiv b \bmod n$ is about a relation between a and b.
- $a = b \bmod n$ means a is *the* remainder of b when divided by n.
- So $-3 \equiv 9 \bmod 6$.
- But $-3 \neq 9 \bmod 6$.
- Instead, $3 = 9 \bmod 6$.

Elementary Facts about Arithmetics in $\mathbb{Z}_n$

- In $\mathbb{Z}_n$, all arithmetics are modulo n.
  - $5 + 6 \equiv 2 \bmod 3$, and $5 \times 7 \equiv 2 \bmod 3$.
- If $f(x_1, x_2, \ldots, x_n)$ is a polynomial with integer coefficients and $a_j \equiv b_j \bmod m$ for $1 \leq j \leq n$, then

$$f(a_1, a_2, \ldots, a_n) \equiv f(b_1, b_2, \ldots, b_n) \bmod m.$$

  - $9^9 \bmod 4 \equiv (9 \bmod 4)^9 \equiv 1 \bmod 4$.

A Key Algorithm

- We are given two integers m, n.
- In many important applications, we need to find integers m' and n' such that

$$mm' + nn' = \gcd(m, n).$$

- This is called the **extended Euclidean algorithm** or **Bézout's identity**.[a]

[a] Bézout (1779).

Extended Euclidean Algorithm

$(u_1, u_2, u_3) := (1, 0, m);$

$(v_1, v_2, v_3) := (0, 1, n);$

while $v_3 \neq 0$ **do**

  $q := \lfloor u_3 / v_3 \rfloor;$

  $(t_1, t_2, t_3) := (u_1 - q v_1, u_2 - q v_2, u_3 - q v_3);$

  $(u_1, u_2, u_3) := (v_1, v_2, v_3);$

  $(v_1, v_2, v_3) := (t_1, t_2, t_3);$

end while

$m' := u_1;$

$n' := u_2;$

$\text{gcd} := u_3;$

return $(m', n', \text{gcd});$

An Example: $n = 100$ and $m = 17$

q	u_1	u_2	u_3	v_1	v_2	v_3
–	1	0	100	0	1	17
5	0	1	17	1	−5	15
1	1	−5	15	−1	6	2
7	−1	6	2	8	−47	1
2	8	−47	1	−17	100	0

We conclude that

$$100 \times 8 + 17 \times (-47) = 1,$$

which is true.

Inverses in $(\mathbb{Z}_n, \times)$

- The x that solves $ax \equiv 1 \bmod n$ is a's **inverse**.
- It is often denoted by $a^{-1} \bmod n$.
- $\gcd(a, n) = 1$ is necessary to solve $ax \equiv 1 \bmod n$.
  - $\gcd(a, n) > 1$ implies $\gcd(ax, n) > 1$ for $x \not\equiv 0 \bmod n$.
  - That makes $ax \equiv 1 \bmod n$ unsolvable.[a]

---

[a]Prove it.

Inverses in $(\mathbb{Z}_n, \times)$ (continued)

- It is also sufficient to solve $ax \equiv 1 \bmod n$.
  - The extended Euclidean algorithm yields two integers a' and n' such that
$$aa' + nn' = 1.$$
  - This implies $aa' \equiv 1 \bmod n$.
  - Thus $x = a'$ is a solution.

Inverses in $(\mathbb{Z}_n, \times)$ (continued)

- The solution to $ax \equiv 1 \bmod n$ is unique modulo n.[a]
  - Suppose there are two solutions x', x''.
  - Then
$$\begin{aligned} ax' &\equiv 1 \bmod n, \\ ax'' &\equiv 1 \bmod n. \end{aligned}$$
  - This implies that $a(x' - x'') \equiv 0 \bmod n$.
  - Hence $n \,|\, a(x' - x'')$.
  - Because $\gcd(a, n) = 1$, we have $n \,|\, (x' - x'')$.
  - It must be that $x' \equiv x'' \bmod n$.

[a] Recall also Theorem 102 (p. 769).

Inverses in $(\mathbb{Z}_n, \times)$ (concluded)

- The inverse $a^{-1} \bmod n$ is hence unique.
- $a^{-1} \bmod n$ has nothing to do with $1/a \in \mathbb{Q}$.
  - Indeed, $1/a$ is in general not even an integer.

The Chinese Remainder Theorem

- Let $n = n_1 n_2 \cdots n_k$, where n_i are pairwise relatively prime.
- Then for any integers $a_1, a_2, \ldots, a_k$, the set of simultaneous equations

$$
\begin{aligned}
x &\equiv a_1 \bmod n_1, \\
x &\equiv a_2 \bmod n_2, \\
&\vdots \\
x &\equiv a_k \bmod n_k,
\end{aligned}
$$

has a unique solution modulo n for the unknown x.

The Chinese Remainder Theorem (concluded)

- The solution can be expressed as a formula.
- Let $m_i = n/n_i$ for $i = 1, 2, \ldots, k$.[a]
- The desired solution is

$$x = a_1 c_1 + a_2 c_2 + \cdots + a_k c_k \bmod n,$$

(remainder after division by n), where

$$c_i = m_i (m_i^{-1} \bmod n_i)$$

for $i = 1, 2, \ldots, k$.

[a] As $m_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$, we have $m_i \equiv 0 \bmod n_j$ for $i \neq j$.

An Example

- Let $n = 5 \times 13 = 65$.
- Hence $n_1 = 5, n_2 = 13, m_1 = 13, m_2 = 5$.
- Consider the equations

$$\begin{aligned} x &\equiv 2 \bmod 5, \\ x &\equiv 3 \bmod 13. \end{aligned}$$

- Hence $a_1 = 2, a_2 = 3$.

An Example (continued)

- Now verify that

$$
\begin{aligned}
13^{-1} &\equiv 2 \bmod 5, \\
5^{-1} &\equiv 8 \bmod 13.
\end{aligned}
$$

  - Indeed,

$$
\begin{aligned}
13 \cdot 2 &\equiv 1 \bmod 5, \\
5 \cdot 8 &\equiv 1 \bmod 13.
\end{aligned}
$$

An Example (concluded)

- Hence the solution is

$$
\begin{aligned}
& 2 \times [\,13 \times (13^{-1} \bmod 5)\,] + 3 \times [\,5 \times (5^{-1} \bmod 13)\,] \\
= \;& 2 \times (13 \times 2) + 3 \times (5 \times 8) \\
= \;& 2 \times 26 + 3 \times 40 \\
= \;& 172 \\
\equiv \;& 42 \bmod 65.
\end{aligned}
$$

- It is easy to confirm that

$$
\begin{aligned}
42 &\equiv 2 \bmod 5, \\
42 &\equiv 3 \bmod 13.
\end{aligned}
$$

Groups, Coding Theory, and Polya's Method of Enumeration

The pursuit of mathematics is a
divine madness of the human spirit.
— Alfred North Whitehead (1861–1947),
Science and the Modern World

Group Theory[a]

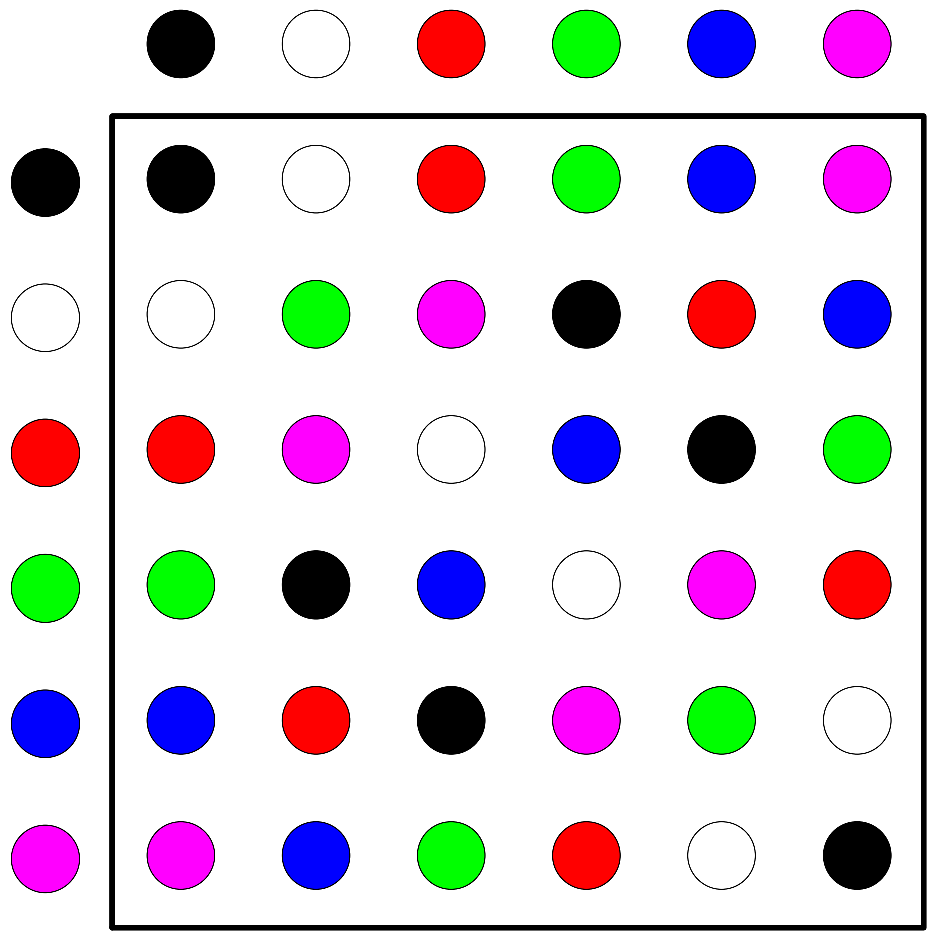
- Let $G \neq \emptyset$ be a set and $\circ$ be a binary operation on G.
- $(G, \circ)$ is called a **group** if it satisfies the following.
  1. For all $a, b \in G$, $a \circ b \in G$ (**closure**).
  2. For all $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$ (**associativity**).
  3. There exists $e \in G$ with $a \circ e = e \circ a = a$ for all $a \in G$ (**identity** or **unit element**).
  4. For each $a \in G$, there is an element $b \in G$ such that $a \circ b = b \circ a = e$ (**inverse**).
- G is **commutative** or **abelian** if $a \circ b = b \circ a$ for all $a, b \in G$.

---

[a] Niels Henrik Abel (1802–1829) and Evariste Galois. This formal definition is by Cayley (1854).

Niels Henrik Abel (1802–1829)

Finite Group as a Table



A Loose End in Item 4?[a]

- Can a "right" inverse be different from a "left" inverse?
- Suppose $a \circ b = e$ and $b' \circ a = e$.
  - b is a right inverse of a.
  - b' is a left inverse of a.
- Then

$$b' = b' \circ e = b' \circ (a \circ b) = (b' \circ a) \circ b = e \circ b = b.$$

- They are identical.

[a]Contributed by Mr. Bao (B90902039) on December 23, 2002.

Examples of Groups

- Under ordinary $+$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are groups.
  - The inverse of a is simply $-a$, which exists.
- Under ordinary $+$, $(\mathbb{N}, +)$ is not a group.
  - The inverse of $a \in \mathbb{Z}^+$ does not exist.
- Under ordinary $\times$, none of $(\mathbb{Z}, \times)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$, and $(\mathbb{C}, \times)$ are groups.
  - The number 0 has no inverses.

Examples of Groups (concluded)

- Under ordinary $\times$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, and $(\mathbb{C}^*, \times)$ are groups if A^* denotes the *nonzero* elements of A.
- Under ordinary $-$, none of $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, and $(\mathbb{R}, -)$ are groups.
  - The associative axiom fails: $a - (b - c) \neq (a - b) - c$.
- $(\mathbb{Z}_n, +)$ is an abelian group for $n > 1$.
- For all $n \in \mathbb{Z}^+$, $|\,(\mathbb{Z}_n, +)\,| = n$.
- But $(\mathbb{Z}_n, \times)$ may not be a group for $n > 1$.[a]

[a] See pp. 803–804.

The Group $(\mathbb{Z}_n^*, \times)$

- Let $\mathbb{Z}_n^*$ stand for the set of positive integers between 1 and $n-1$ that are relatively prime to n.
- $(\mathbb{Z}_n^*, \times)$ is a (multiplicative) abelian group.
  - Here, $\times$ is done modulo n.[a]
- By definition,[b]

$$\phi(n) \stackrel{\Delta}{=} |\,(\mathbb{Z}_n^*, \times)\,|. \tag{105}$$

  - $\mathbb{Z}_{12}^* = \{\,1, 5, 7, 11\,\}$.
  - Hence $\phi(12) = 4$.

---

[a]Review pp. 786ff for the inverses modulo n.

[b]Recall p. 424.

The Group $(\mathbb{Z}_n^*, \times)$ (concluded)

- In particular, $(\mathbb{Z}_p^*, \times)$ is a (multiplicative) abelian group for prime p.
- For all prime p,

$$|\,(\mathbb{Z}_p^*, \times)\,| = p - 1.$$

  – Note that $p - 1$ is *not* a prime unless $p = 3$.

Rings Redefined

- $(R, +, \cdot)$ is a ring if the following conditions hold.
  - $(R, +)$ is an abelian group.
  - $a \cdot b \in R$ for all $a, b \in R$ (closure).
  - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$ (associativity).
  - $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$ (distributive laws of $\cdot$ over $+$).

Properties of Groups[a]

- The identity of G is unique.[b]
  - If e_1, e_2 are both identities, then
$$e_1 = e_1 \circ e_2 = e_2$$
    by the identity condition.
- The inverse of each element of G is unique.[c]
  - Suppose b, c are both inverses of $a \in G$.
  - Then $b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c$.

[a] Properties must be proved using only the four axioms or their logical corollaries.

[b] Recall p. 755.

[c] Recall p. 756.

The Cancellation Properties[a]

The left-cancellation property: If $a, b, c \in G$ and $a \circ b = a \circ c$, then $b = c$.

- $b = (a^{-1} \circ a) \circ b = a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) = (a^{-1} \circ a) \circ c = c$.

The right-cancellation property: If $a, b, c \in G$ and $b \circ a = c \circ a$, then $b = c$.

---

[a] Recall Theorem 98 (p. 763).

Inverses[a]

- $(a^{-1})^{-1} = a$.
  - Both are inverses of a^{-1}.
  - But inverse is unique.[b]
- $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.
  - The identity claims $b^{-1} \circ a^{-1}$ is the inverse of $a \circ b$.
  - Indeed,

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ b = e.$$

[a]Contrast them with Corollary 101 (p. 767).

[b]Recall p. 806.

Powers

- The associative property implies that $a_1 \circ a_2 \circ \cdots \circ a_n$ is well-defined.
- For $n > 0$, define

$$a^n = \overbrace{a \circ a \circ \cdots \circ a}^{n}.$$

- For $n < 0$, define

$$a^n = \overbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}^{-n} = \left(a^{-1}\right)^{-n}. \tag{106}$$

  - Note that $(a^{-1})^n = a^{-n}$.
- Define $a^0 = e$.

Powers (concluded)

- $(a^n)^{-1} = (a^{-1})^n$.
  - When $n > 0$,

$$\begin{aligned} a^n \circ \left(a^{-1}\right)^n &= a^{n-1} \circ \boxed{a \circ a^{-1}} \circ \left(a^{-1}\right)^{n-1} \\ &= a^{n-1} \circ \left(a^{-1}\right)^{n-1} \\ &= \cdots = e. \end{aligned}$$

  - When $n < 0$, by Eq. (106) on p. 809,

$$a^n \circ \left(a^{-1}\right)^n = \left(a^{-1}\right)^{-n} \circ \left(\left(a^{-1}\right)^{-1}\right)^{-n},$$

    which equals e by the same argument above.

Operations on Powers

Lemma 106 *$a^n \circ a^m = a^{n+m}$ for $n, m \in \mathbb{Z}$.*

- For $n, m \geq 0$,

$$a^n \circ a^m = \overbrace{a \circ \cdots \circ a}^{n} \circ \overbrace{a \circ \cdots \circ a}^{m} = \overbrace{a \circ \cdots \circ a}^{n+m} = a^{n+m}.$$

- For $n \geq 0, m < 0$, and $-m \leq n$,

$$\begin{aligned} a^n \circ a^m &= \overbrace{a \circ \cdots \circ a}^{n} \circ \overbrace{a^{-1} \circ \cdots \circ a^{-1}}^{-m} = \overbrace{a \circ \cdots \circ a}^{n-1} \circ \overbrace{a^{-1} \circ \cdots \circ a^{-1}}^{-m-1} \\ &= \cdots = \overbrace{a \circ \cdots \circ a}^{n-(-m)} = \overbrace{a \circ \cdots \circ a}^{n+m} = a^{n+m}. \end{aligned}$$

- The other cases are similar.

Subgroups

- Let $(G, \circ)$ be a group.
- Let $\emptyset \neq H \subseteq G$.
- If H is a group under $\circ$, we call it a **subgroup** of G.
- For example, the set of even integers is a subgroup of $(\mathbb{Z}, +)$.[a]
- H "inherits" $\circ$ from G: It produces the same results as in G.
- $\{ e \}$ and G are the two **trivial** subgroups of G.

[a] Prove it.

Criteria for Being a Subgroup

Only two axioms out of four need to be checked.

Theorem 107 *Let H be a nonempty subset of a group $(G, \circ)$. Then H is a subgroup of G if and only if (1) for all $a, b \in H$, $a \circ b \in H$ (closure), and (2) for all $a \in H$, $a^{-1} \in H$ (inverse).*

Proof ($\Rightarrow$):

- Assume that H is a subgroup of G.
- Then H is a group.
- So H satisfies, among other things, the closure axiom (1) and the inverse axiom (2).

The Proof (concluded)

Proof ($\Leftarrow$):

- Let $H \neq \emptyset$ satisfy (1) and (2).
- We need to verify the associative axiom and the existence of identity for H.
  - **Associativity:** For all $a, b, c \in H$, $(a \circ b) \circ c = a \circ (b \circ c) \in G$, hence in H by (1).
  - **Identity:** For any arbitrary $a \in H$, $a^{-1} \circ a \in H$ by (1) and (2) and is the identity.

Simpler Criterion for Being a Subgroup

Theorem 108 *Let H be a nonempty subset of a group $(G, \circ)$. Then H is a subgroup of G if and only if $a \circ b^{-1} \in H$ for all $a, b \in H$.*

Proof ($\Rightarrow$):

- Obvious by the axioms of group theory.

Proof ($\Leftarrow$):

- First, $a \circ a^{-1} \in H$ for any $a \in H$.
- Hence
$$e = a \circ a^{-1} \in H.$$

The Proof (concluded)

- By Theorem 107 (p. 813), we only need to prove the closure and inverse axioms hold.
- **Closure:** For any arbitrary $a, b \in H$,

$$a \circ b = a \circ (b^{-1})^{-1} \in H.$$

- **Inverse:** For any $b \in H$,

$$b^{-1} = e \circ b^{-1} \in H.$$

