GROUP THEORY

Haiyang Yu

01/14/2018

Outline

- Historical origin of group theory
- Number theory
- Abstract (modern) algebra
- Applications

- 9^{th} century: junior algebra
- 16^{th} century: cubic equation and fourth degree equation
- 18^{th} century: Lagrange's contributions
- 19^{th} century: Galois theory
- Abstract (modern) algebra

Historical origin of group theory

The concept of “algebra”

- Arithmetic versus algebra
  - E.g. 5+7=12 (arithmetic); a+b=c (algebra)
- Algebra is the abstract form of arithmetic
- The word “algebra” comes from the name of a treatise of the mathematician and astronomer Mahommed ibn Musa al-Kharizmi (Mahommed, son of Musa, native of Kharizm) in the 9th century
- His treatise on algebra was called “Al-jebr al-muqabala”, which means “transposition and removal”
  - Transposition (al-jebr): transfer of native terms to the other side of an equation
  - Removal (al-muqabala): cancellation of equal terms
- The Arabic word “al-jebr” → “algebra” (Latin)

Linear and quadratic equations

- Up to the 19th century, the majority of "algebra" had been dealing with equations, especially finding the roots of a polynomial equation:

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0,$$

- First-degree

$$x + a = 0 \qquad\qquad x = -a.$$

- Second-degree

$$x^2 + px + q = 0 \qquad\qquad x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Third-degree (cubic) equation

- Beginning of 16th century: in the era of the Renaissance, solved by the Italian mathematician Scipio del Ferro.
- Then: Tartaglia (1500-1557), Cardan (1501-1576)

Scipio del Ferro. Del Ferro, following the custom of his time, did not publish his own discoveries but communicated them to one of his pupils. After the death of del Ferro this pupil challenged to competition one of the great Italian mathematicians Tartaglia and proposed to him for solution a series of third-degree equations. Tartaglia (1500–1557) accepted the challenge and eight days before the end of the competition found a method of solving any cubic equation of the form $x^3 + px + q = 0$.

Third-degree (cubic) equation

- Cardan's formula

In two hours he solved all problems of his opponent. A professor of physics and mathematics in Milan, Cardan (1501–1576), learning of Tartaglia's discoveries, began to entreat Tartaglia to inform him of his secret. Tartaglia finally agreed, but with the condition that Cardan keep his method in deep secret. Cardan violated his promise and published Tartaglia's result in his work "The great art" ("*Ars Magna*").

The formula for the solution of a cubic equation has since then been called Cardan's formula, although it would be correct to call it Tartaglia's formula.

In the first place, the solution of the general cubic equation

$$y^3 + ay^2 + by + c = 0$$

can easily be reduced to the solution of the cubic equation of the form

$$x^3 + px + q = 0,$$

Hint: set $y = x - a/3$.

Let:

$$x = u + v$$
$$uv = -\frac{p}{3}$$

$$u^3 + v^3 + q = 0,$$
$$3uv + p = 0.$$

$$u^3 + v^3 = -q,$$
$$u^3 v^3 = -\frac{p^3}{27}$$

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Fourth-degree equation

- 4-d equations were solved by Ferrari (1522-1565)

$$x^4 + ax^3 + bx^2 + cx + d = 0.$$

Let us rewrite it as:

$$x^4 + ax^3 = -bx^2 - cx - d$$

and add to both sides $a^2x^2/4$; then on the left we obtain a perfect square

$$\left(x^2 + \frac{ax}{2}\right)^2 = \left(\frac{a^2}{4} - b\right)x^2 - cx - d.$$

Adding now to both sides of the equation the terms

$$\left(x^2 + \frac{ax}{2}\right)y + \frac{y^2}{4},$$

where y is a new variable, on which we later impose a necessary condition, on the left we obtain a perfect square

$$\left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=\left(\frac{a^2}{4}-b+y\right)x^2+\left(\frac{ay}{2}-c\right)x+\left(\frac{y^2}{4}-d\right).$$

Thus we have reduced the problem to one with two unknowns.

if we select y such that

$$\left(\frac{ay}{2}-c\right)^2-4\left(\frac{a^2}{4}-b+y\right)\left(\frac{y^2}{4}-d\right)=0$$

, which is a cubic equation of y that can be solved by Cardan's formula:

$$y^3-by^2+(ac-4d)y-[d(a^2-4b)+c^2]=0.$$

Then, the right hand side of the original equation becomes a complete square form:

$$\left(x^2+\frac{ax}{2}+\frac{y_0}{2}\right)^2=(\alpha x+\beta)^2$$

$$x^2+\frac{ax}{2}+\frac{y_0}{2}=\alpha x+\beta \quad \text{or} \quad x^2+\frac{ax}{2}+\frac{y_0}{2}=-\alpha x-\beta$$

, where y0, alpha, beta are solved from the above cubic equation of y.

Viete's formula

- Short description: represent coefficients with roots rationally

Consider the general form: $f(x) = 0,$

where $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$

Then, the polynomial f(x) can be represented (and in only one way) as:

$$f(x) = (x - a)(x - b) \cdots (x - l),$$

where $a, b, \cdots, l$ are real or complex numbers. (roots of the equation)

$$\begin{aligned} -a_1 &= a + b + c + \cdots + l, \\ a_2 &= ab + ac + \cdots + kl, \\ -a_3 &= abc + abd + \cdots, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \pm a_n &= abc \cdots l \end{aligned}$$

The order of roots doesn't change the representing of coefficients: symmetric polynomials

Lagrange resolvent

1770-1771: “Reflections on the solution of algebraic equations”

In his investigations, Lagrange introduced the expression

$$a + \epsilon b + \epsilon^2 c + \cdots + \epsilon^{n-1} l$$

in the roots a, b, $\cdots$, l of an equation, where ϵ is an nth root of unity,* having established that such expressions are closely connected with the solution of equations by radicals. These expressions are now called “Lagrange resolvents.”

In addition, Lagrange observed that the theory of permutations of roots of an equation is of great importance in the theory of solution of equations. He even expressed the thought that the theory of permutations is the “true philosophy of the whole question,” in which he was completely right, as was shown in the later investigations of Galois.

Let us consider, for example, the solution by Lagrange's method of the general fourth-degree equation

$$x^4 + mx^3 + nx^2 + px + q = 0.$$

Let the roots of this equation be a, b, c, d. Consider the resolvent

$$a + b - c - d,$$

i.e.,

$$a + \epsilon c + \epsilon^2 b + \epsilon^3 d,$$

where $\epsilon = -1$. If we permute a, b, c, d in all $1 \cdot 2 \cdot 3 \cdot 4 = 24$ different ways, we obtain altogether six different expressions

$$\begin{aligned} &a + b - c - d, \\ &a + c - b - d, \\ &a + d - c - b, \\ &c + d - a - b, \\ &b + d - a - c, \\ &b + c - a - d. \end{aligned} \tag{5}$$

An equation of the sixth-degree, whose roots are these six expressions, will thus have coefficients that do not vary with all 24 permutations of a, b, c, d, since any of the 24 permutations can only permute these expressions among themselves and the coefficients of the sixth-degree equation do not depend on the order in which we take its roots. Thus, these coefficients are symmetric polynomials in a, b, c, d. But then, by virtue of the fundamental theorem on symmetric polynomials, these coefficients are expressed integral rationally in terms of the coefficients m, n, p, q of the equation. In addition, since expressions (5) are pairwise of opposite signs, this sixth-degree equation will contain only terms of even powers. Indeed, if expressions (5) are denoted by α, β, γ, $-\alpha$, $-\beta$, $-\gamma$ respectively, then the left-hand side of the sixth-degree equation will be equal to

$$(y-\alpha)(y+\alpha)(y-\beta)(y+\beta)(y-\gamma)(y+\gamma) = (y^2-\alpha^2)(y^2-\beta)(y_2-\gamma^2).$$

Direct computation gives the sixth-degree equation

$$y^6-(3m^2-8n)y^4+3(m^4-16m^2n-16n^2+16mp-64q)y^2 - (m^2-4m+8p)^2=0.$$

Coefficients

$$x^4 + mx^3 + nx^2 + px + q = 0.$$

Roots

$$-m = a + b + c + d$$

$$n = ab + ac + ad + bc + bd + cd$$

$$-p = abc + abd + acd + bcd$$

$$q = abcd$$

$$\alpha = a + b - c - d$$

$$\beta = a + c - b - d$$

$$\gamma = a + d - c - b$$

$$-\alpha = c + d - a - b$$

$$-\beta = b + d - a - c$$

$$-\gamma = c + b - a - d$$

$$\left(y^2 - \alpha^2\right)\left(y^2 - \beta^2\right)\left(y^2 - \gamma^2\right) = 0$$

Letting $y^2 = \mathrm{t}$, we obtain a cubic equation in t, and if t', t'', t''' are its roots, then

$$a + b - c - d = \sqrt{t'},$$

$$a + c - b - d = \sqrt{t''},$$

$$a + d - b - c = \sqrt{t'''}.$$

We also have

$$a + b + c + d = -m.$$

Adding these equations after multiplication by 1, 1, 1, 1 or 1, -1, -1, 1, or -1, 1, -1, 1, or -1, -1, 1, 1, we obtain

$$a = \frac{1}{4}(-m + \sqrt{t'} + \sqrt{t''} + \sqrt{t'''}),$$

$$b = \frac{1}{4}(-m + \sqrt{t'} - \sqrt{t''} - \sqrt{t'''}),$$

$$c = \frac{1}{4}(-m - \sqrt{t'} + \sqrt{t''} - \sqrt{t'''}),$$

$$d = \frac{1}{4}(-m - \sqrt{t'} - \sqrt{t''} + \sqrt{t'''}).$$

19th century

- Abel (1802-1829)

Abel's discovery. Consequently it was a great surprise to all mathematicians when in 1824 the work of a young Norwegian genius Abel (1802–1829) came to light, in which a proof was given that if the coefficients of an equation $a_1, a_2, \cdots, a_n$ are regarded simply as letters, then there does not exist any radical expression in these coefficients that is a root of the corresponding equation, if its degree $n \geqslant 5$. Thus, for three centuries the efforts of the greatest mathematicians of all countries to solve equations of degree 5 or higher in radicals did not lead to success for the simple reason that this problem simply does not have a solution.

Such a formula is known for second-degree equations, and as we saw analogous formulas exist for third- and fourth-degree equations, but for equations of degree 5 or greater there are no such formulas.

Abel's proof is difficult and we will not give it here.

19th century

- In face, there are many special equations that can be solved in radicals, which Abel couldn't explain why, for example, Gauss proposed the "cyclotomic" equations (p is a prime number):

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = 0,$$

Thus, after Abel's work the situation was the following: Although, as was shown by Abel, the general equation of degree higher than 4 cannot be solved by radicals, there are arbitrarily many different special equations of arbitrary degree, all of which can be solved by radicals. The whole question of solving equations in radicals was placed by these discoveries on completely new ground. It became clear that the task now was to determine exactly which equations can be solved by radicals, or in other words, what are the necessary and sufficient conditions for the solvability of an equation in radicals. This problem, the answer to which gave in some sense the final elucidation of the whole problem, was solved by the ingenious French mathematician Evariste Galois.

Galois (1811-1832) theory

- https://en.wikipedia.org/wiki/%C3%89variste_Galois
- Established group theory, concept of "field"
- Connected the algebraic solution to a polynomial equation to the structure of a group of permutations associated with the roots of the polynomial, the Galois group of the polynomial
- He found that an equation could be solved in radicals if one can find a series of subgroups of its Galois group, each one normal in its successor with Abelian quotient, or its Galois group is solvable

A portrait of Évariste Galois aged about 15

Abstract (modern) algebra

- Axiomatization of algebra
  - Generalization of numbers
  - Integer → algebraic integer
  - Complex numbers → hyper-complex numbers, Klein four-group
- Algebra v.s. geometry
  - Connection between “symmetries” of geometries and properties of groups → quantum mechanics, crystal theory
  - Vector space: transformation matrix with invariants (e.g. distance, area) → Klein geometries
  - Continuous groups, differential equations → Lie group, Lie algebra

- Divisibility, prime, gcd, lcm
- Euclidean algorithm
- Diophantine equation
- Congruences and congruence equation
- Chinese remainder theorem

Number theory

Divisibility, prime, gcd, lcm

- Let x and y are integers ($x \neq 0$), if y/x is an integer, then we say:
  - x divides y
  - y is divisible by x
  - x is a divisor or factor of y
  - y is a multiple of x
- Prime number: the only positive divisors are 1 and itself
- Composite: not prime number

An integer n is divisible:

There is no simple test for divisibility by 7.

- by 2, if and only if the units digit of n is 0, 2, 4, 6, or 8.

  For example, 1358 is divisible by 2, but 2467 is not.

- by 3, if and only if the sum of the digits of n is itself divisible by 3.

  For example, 28554 is divisible by 3 since $2 + 8 + 5 + 5 + 4 = 24$ is divisible by 3.

- by 4, if and only if the number formed by the last two digits of n is divisible by 4.

  For example, 139756 is divisible by 4 because 56 is divisible by 4.

- by 5, if and only if the units digit of n is 0 or 5.

  For example, 4085 is divisible by 5, but 5804 is not.

- by 6, if and only if n is divisible by both 2 and 3.

  For example, 6498 is divisible by 6 since it's even and $6 + 4 + 9 + 8 = 27$ is divisible by 3.

- by 8, if and only if the number formed by the last three digits of n is divisible by 8.

  For example, 4895064 is divisible by 8 since $064 = 64$ is divisible by 8.

- by 9, if and only if the sum of the digits of n is itself divisible by 9.

  For example, 4895064 is divisible by 9 since $4 + 8 + 9 + 5 + 0 + 6 + 4 = 36$ is divisible by 9.

- Relatively prime (or coprime): if the only positive divisor they have in common is 1.
- Division algorithm: if x and y are positive integers (a≠0), then we can find unique integers q and r such that:
- y = q*x + r, where 0 ≤ r < x
- Here, we call q the quotient and r the remainder
- Fundamental theorem of arithmetic: every integer n>1 can be expressed as a unique product of primes.
  - E.g. $3960 = 2^3 * 3^2 * 5 * 11$
- The great common divisor (gcd) and the least common multiple (lcm)

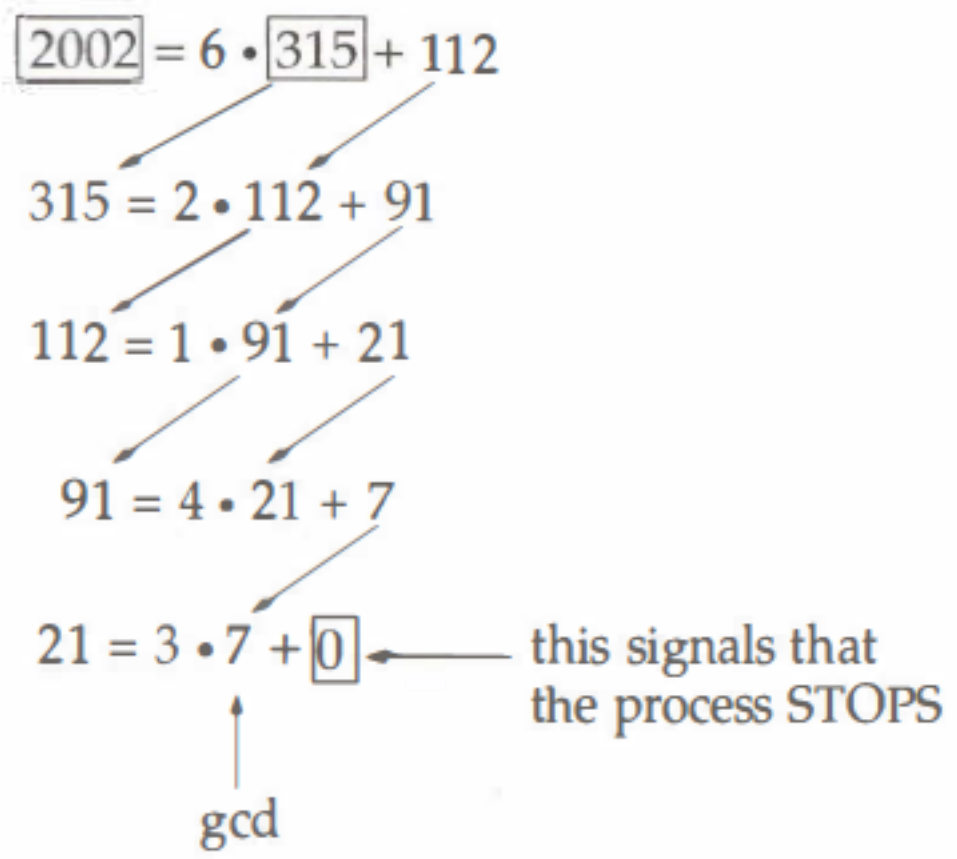
$$a = (p_1)^{a_1}(p_2)^{a_2}\cdots(p_k)^{a_k} \quad \text{and} \quad b = (p_1)^{b_1}(p_2)^{b_2}\cdots(p_k)^{b_k}$$

$$m_i = \min(a_i, b_i) \quad \text{and} \quad M_i = \max(a_i, b_i)$$

$$\gcd(a, b) = (p_1)^{m_1}(p_2)^{m_2}\cdots(p_k)^{m_k} \quad \text{and} \quad \operatorname{lcm}(a, b) = (p_1)^{M_1}(p_2)^{M_2}\cdots(p_k)^{M_k}$$

Euclidean algorithm

- What is the great common divisor of 2002 and 315?



The Diophantine equation

- a*x + b*y = c
- All the variables are restricted to integers
  - E.g. x+2y = 3, what are the integer solutions?
  - Ans: one solution is (1, 1), the general solutions are: (1+2t, 1-t)
- Requirement: gcd(a,b) should divide c, otherwise there will be no integral solution
- Fermat's last theorem: $x^n + y^n = z^n$, if the integer n>2, this equation has no solutions in nonzero integers x, y, and z.
- How to solve a linear Diophantine equation: ax + by = c?
  - 1. Find one solution: (x_0, y_0)
  - 2. Get the general solutions: (x0 + (b/d)t, y0 - (a/d)t), where d is gcd(a, b), t is any integer.
  - Qu: gcd(a, b) is easy to find, but how to find one solution (x_0, y_0)?

The Diophantine equation

- Let consider an example: 15x + 49y = 8
- gcd(15, 49) = 1, which divides 8, so this equation has infinite integral solutions

Euclidean algorithm

$$49 = 3 \cdot 15 + 4$$
$$15 = 3 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

gcd(15,49)

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ &= 4 - (15 - 3 \cdot 4) \cdot 1 \\ &= 4 \cdot 4 - 15 \\ &= 4 \cdot (49 - 3 \cdot 15) - 15 \\ &= 15 \cdot (-13) + 49 \cdot (4) \end{aligned}$$

$$15 \cdot (-104) + 49 \cdot (32) = 8$$

$$x = -104 + 49t \quad \text{and} \quad y = 32 - 15t$$

Congruences

- $a \equiv b \pmod{n}$: a is congruent to b modulo n if a-b is divisible by n

1. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
2. If $a \equiv b \pmod{n}$, then for any c,

   $$a \pm c \equiv b \pm c \pmod{n}$$

   $$ac \equiv bc \pmod{n}$$
3. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

   $$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n}$$

   $$a_1 a_2 \equiv b_1 b_2 \pmod{n}$$
4. For any positive integer c, the statement $a \equiv b \pmod{n}$ is equivalent to the congruences $a \equiv b$, $b + n$, $b + 2n$, . . . , $b + (c - 1)n \pmod{cn}$.
5. If $ab \equiv ac \pmod{n}$, then

   $b \equiv c \pmod{n}$ if $\gcd(a, n) = 1$

   $b \equiv c \pmod{\frac{n}{d}}$ if $d = \gcd(a, n) > 1$
6. **Fermat's Little theorem**. If p is a prime and a is an integer, then

   $a^{p-1} \equiv 1 \pmod{p}$, if p does not divide a

   $a^p \equiv a \pmod{p}$, for any integer a

Example 6.4 What's the remainder when 2^{345} is divided by 29?

Solution: Since 29 is a prime, Fermat's little theorem tells us that $2^{28} \equiv 1 \pmod{29}$.
Since $2^{345} = (2^{28})^{12} \cdot 2^9$, we can conclude that $2^{345} = (2^{28})^{12} \cdot 2^9 \equiv 1^{12} \cdot 2^9 \equiv 2^9 \pmod{29}$.
Now, since $2^5 \equiv 3 \pmod{29}$, we have $2^9 = 2^5 \cdot 2^4 \equiv 3 \cdot 2^4 = 48 \equiv 19 \pmod{29}$.
Therefore, when 2^{345} is divided by 29, the remainder will be 19.

The congruence equation

- $ax \equiv b \pmod{n}$, where $a \neq 0$

7. The linear congruence equation $ax \equiv b \pmod{n}$ has a solution if and only if $d = \gcd(a, n)$ divides b, and

   if $d = 1$, then the solution is unique $\pmod{n}$

   if $d > 1$, then the solution is unique $\left(\mod \frac{n}{d}\right)$

  - E.g. $2x \equiv 5 \pmod{6}$ has no solution
- Algorithm 1: $ax \equiv b \pmod{n}$ can be reduced into a linear Diophantine equation $a*x - n*k = b$, where k is an integer, which is solvable.
- Algorithm 2: recursive method

Example 6.5 There's only one integer, x, between 100 and 200 such that $144x \equiv 22 \pmod{71}$. What's x?

Example 6.5 There's only one integer, x, between 100 and 200 such that $144x \equiv 22 \pmod{71}$. What's x?

Solution: Let's solve the linear congruence equation by the following steps:

$$144x \equiv 22 \pmod{71}$$

$$144x \equiv 93 \pmod{71} \quad \text{[adding the congruence } 0 \equiv 71 \pmod{71}\text{]}$$

$$48x \equiv 31 \pmod{71} \quad \text{[dividing both sides by 3]}$$

$$48x \equiv -40 \pmod{71} \quad \text{[adding the congruence } 0 \equiv -71 \pmod{71}\text{]}$$

$$6x \equiv -5 \pmod{71} \quad \text{[dividing both sides by 8]}$$

$$6x \equiv 66 \pmod{71} \quad \text{[adding the congruence } 0 \equiv 71 \pmod{71}\text{]}$$

$$x \equiv 11 \pmod{71} \quad \text{[dividing both sides by 6]}$$

Therefore, the positive values of x that satisfy the equation are:

$$11, \quad 11 + 71 = 82, \quad 11 + 2 \cdot 71 = 153, \quad 11 + 3 \cdot 71 = 224, \ldots \text{etc.}$$

The only integer between 100 and 200 that satisfies this condition is $x = 153$.

Chinese remainder theorem

- The earliest known statement of the theorem, as a problem with specific numbers, appears in the 3rd century book *Sunzi Suanjing* by the Chinese mathematician Sunzi:
- "There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?"
- In mathematical language, it is:

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7$$

What is the solution of x?

$$x \equiv 2 \pmod 3 \quad x + 3i = 2 \quad x = -1 + 3n_1,\ i = 1 - n_1$$

$$x \equiv 3 \pmod 5 \Rightarrow x + 5j = 3 \Rightarrow x = -2 + 5n_2,\ j = 1 - n_2$$

$$x \equiv 2 \pmod 7 \quad x + 7k = 2 \quad x = -5 + 7n_3,\ k = 1 - n_3$$

$$\Rightarrow \begin{matrix} 5n_2 - 3n_1 = 1 \\ 7n_3 - 5n_2 = 3 \end{matrix} \Rightarrow \begin{matrix} n_2 = -1 + 3m_1,\ n_1 = -2 + 5m_1 \\ n_3 = -1 + 5m_2,\ n_2 = -2 + 7m_2 \end{matrix}$$

$$\Rightarrow 7m_2 - 3m_1 = 1 \Rightarrow m_2 = 1 + 3p,\ m_1 = 2 + 7p$$

$$\Rightarrow \begin{matrix} n_1 = 8 + 35p \\ n_2 = 5 + 21p \\ n_3 = 4 + 15p \end{matrix} \Rightarrow \boxed{x = 23 + 105p}$$

HW: how to tell if the solutions exist for a given set of equations?

- Group, semi-group, monoid, Abelian group
- Cyclic groups
- Subgroups, cyclic subgroups, generators
- Isomorphism
- Finite Abelian groups
- Homomorphism
- Equivalence, conjugation
- Normal subgroup, coset, quotient group
- Rings
- Fields

Abstract (modern) algebra

Definitions

- A set G together with a binary operation * defined on it is called a group with respect to this operation (G, *) if the following group axioms are satisfied:
  - 1. Closure: for any x, y in G, x*y is still in G;
  - 2. Associativity: for any x, y, z in G, we have
    $$x*(y*z) = (x*y)*z;$$
  - 3. Identity: there exists an element e in G such that for every x in G, we have
    $$x*e = e*x = x;$$
  - 4. Invertibility: for every x in G, there exists an element x^{-1} in G such that
    $$x*x^{-1} = x^{-1}*x = e.$$
- Finite group v.s. infinite group: order of a group
- Abelian group:
  - For any x, y in a group (G, *) (usually just written as G), if x*y = y*x (commutative), this group is called Abelian group.

Group-like structures

	Totality[α]	Associativity	Identity	Invertibility	Commutativity
Semigroupoid	Unneeded	Required	Unneeded	Unneeded	Unneeded
Category	Unneeded	Required	Required	Unneeded	Unneeded
Groupoid	Unneeded	Required	Required	Required	Unneeded
Magma	Required	Unneeded	Unneeded	Unneeded	Unneeded
Quasigroup	Required	Unneeded	Unneeded	Required	Unneeded
Loop	Required	Unneeded	Required	Required	Unneeded
Semigroup	Required	Required	Unneeded	Unneeded	Unneeded
Monoid	Required	Required	Required	Unneeded	Unneeded
Group	Required	Required	Required	Required	Unneeded
Abelian group	Required	Required	Required	Required	Required

^α Closure, which is used in many sources, is an equivalent axiom to totality, though defined differently.

Some notations

$\mathbf{Z}$ = the set of all integers

$\mathbf{Q}$ = the set of all rational numbers (i.e., those real numbers of the form $\frac{a}{b}$, where a and b are integers and $b \neq 0$)

$\mathbf{R}$ = the set of all real numbers

$\mathbf{C}$ = the set of all complex numbers

$M_{m \times n}(S)$ = the set of all $m \times n$ matrices whose entries are in the set S

$M_n(S)$ = the set of all $n \times n$ (square) matrices whose entries are in the set S

Furthermore, a "+" superscript on a set of numbers indicates the subset of *positive* numbers in that set; so $\mathbf{Z}^+$ is the set of positive integers, $\mathbf{Q}^+$ is the set of positive rationals, and $\mathbf{R}^+$ is the set of positive reals. If the "+" superscript is accompanied by an overbar on the set—as in $\overline{\mathbf{Z}}^+$, $\overline{\mathbf{Q}}^+$, and $\overline{\mathbf{R}}^+$—this indicates the subset of all *nonnegative* numbers in that set. So, for example, $\overline{\mathbf{Z}}^+$ is the union of $\mathbf{Z}^+$ and $\{0\}$. And, finally, a "*" superscript on a set of numbers—such as $\mathbf{Z}^*$, $\mathbf{Q}^*$, $\mathbf{R}^*$, or $\mathbf{C}^*$—denotes the subset of all *nonzero* numbers in that set.

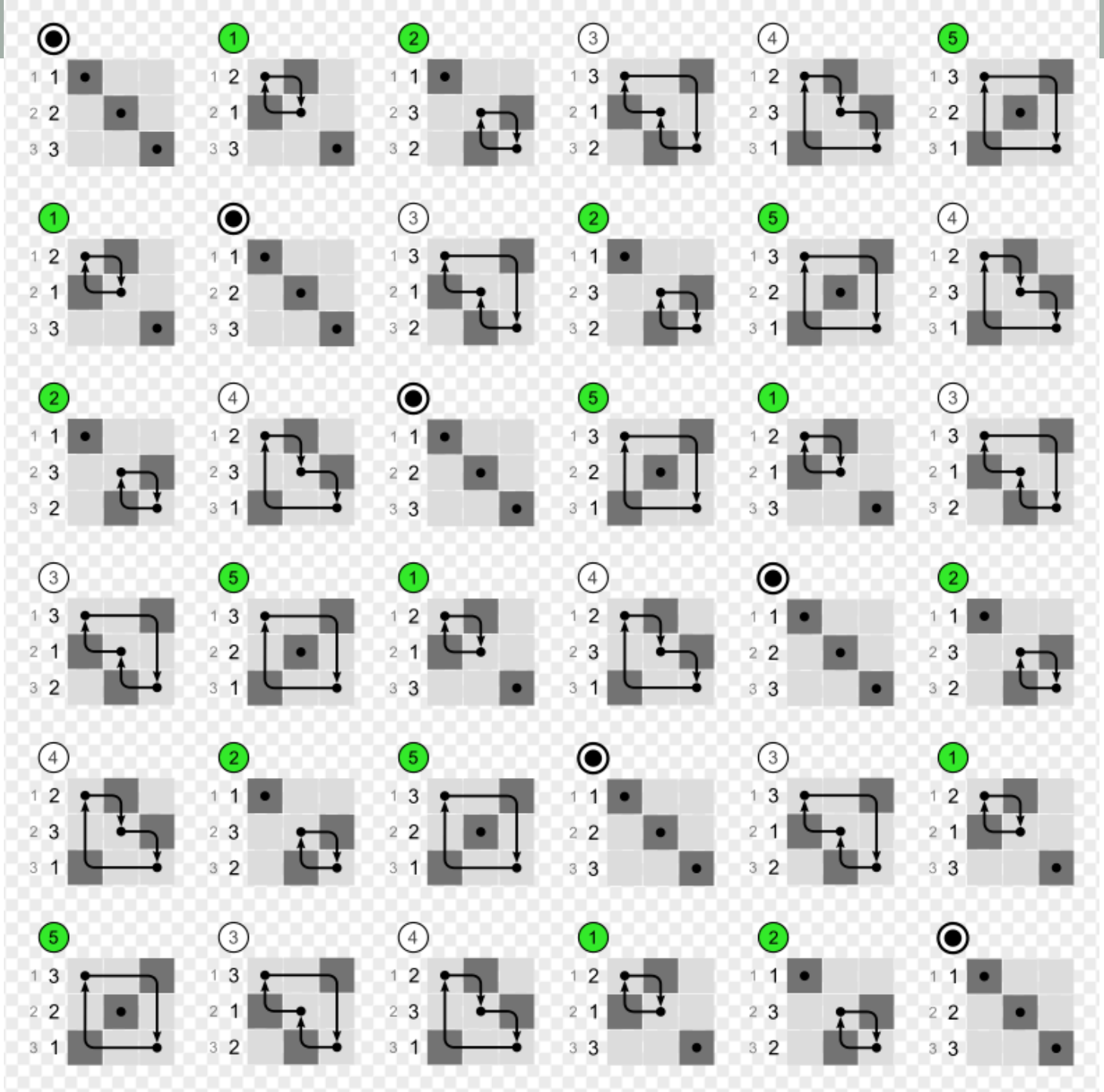
Examples

- Z^+ is closed for addition +, but not closed for subtraction -;
- $(Z^*, \times)$ is not a group, but $(Q^*, \times)$ is a group
- Typical infinite Abelian groups:
  - $(Z, +)$, $(Q, +)$, $(R, +)$, $(C, +)$, $(Q^*, \times)$, $(R^*, \times)$, $(C^*, \times)$
  - $(M_{m\times n}(S), +)$ and $(M_n(S), +)$, where S in Z, Q, R, or C.
- General linear group GL(n, R):
  - Subset of $M_n(R)$ that consists of all invertable n×n matrices with entries in R (or Q, C)
- Special linear group SL(n, R):
  - Subset of GL(n, R), but with determinant being 1.
  - The closure is easily tested: det(AB) = det(A)det(B)
- Group of n^{th} roots of unity: $U_n = \{z: z^n = 1\}$, z is in C;

- Permutation group: symmetric group on n letters S_n:
  - All the permutations (bijective mapping) from the set {1, 2, …, n} to itself; obviously, the order of S_n is n!
  - For every n>=3, S_n is a non-Abelian group

Group multiplication table

S_3	e	(1,2)	(1,3)	(2,3)	(1,2,3)	(1,3,2)
e	e	(1,2)	(1,3)	(2,3)	(1,2,3)	(1,3,2)
(1,2)	(1,2)	e	(1,2,3)	(1,3,2)	(1,3)	(2,3)
(1,3)	(1,3)	(1,3,2)	e	(1,2,3)	(2,3)	(1,2)
(2,3)	(2,3)	(1,2,3)	(1,3,2)	e	(1,2)	(1,3)
(1,2,3)	(1,2,3)	(2,3)	(1,2)	(1,3)	(1,3,2)	e
(1,3,2)	(1,3,2)	(1,3)	(2,3)	(1,2)	e	(1,2,3)



- Additive group of integers modulo n (Z_n, $\oplus$):
  - For any two integers x and y in Z_n, define $a \oplus b$ to be the remainder of a+b being divided by n;
  - It is a finite Abelian group of order n.

group table for $(\mathbf{Z}_6, \oplus)$:

$\oplus$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- Multiplicative group of integers modulo p (Z^*_p, $\otimes$)
  - Z^*_p: set of integers modulo p except 0
  - p should be a prime number, otherwise, some elements will have no inverse.

Group table for (Z^*_5, $\otimes$)

$\otimes$	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Cyclic groups

- If there exists an element a in a group (G, *) such that
$$G = \{a^n : n=0,1,2,\ldots\}$$
- we call this group is cyclic, and the element a is a generator of the group, where $a^0=e$, $a^n = a^{n-1} * a$.
- There could be more than one generator in one group, for example, $U_4 = \{1, i, -1, -i\}$ have two generator i and −i;
- Theorem: the integer m is a generator of $(Z_n, \oplus)$ if and only if m is relatively prime to n.
  - E.g. $(Z_n, \oplus)$ is generated by 1 and 5, but not 2, 3, 4.
- Theorem: if a is a generator of group G with order n, then the element a^m is also a generator of G if and only if m is relatively prime to n.
  - E.g. for U_4, i is a generator, $i^3 = -i$ is also a generator.

- Theorem: every cyclic group is Abelian, but not every Abelian group is cyclic.
  - Proof: let a is a generator, then $a^m * a^n = a^{m+n} = a^n * a^m$
  - E.g. Klein four-group V_4: it is an Abelian group, but not cyclic (no generator exist)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Subgroups, cyclic subgroups

- Let (G, *) is a group, if there exists a subset H of G such that (H, *) is also a group, then H is a subgroup of G.
  - E.g. {e} and G itself are subgroups of G
  - E.g. {e, a}, {e, b}, {e, c} are subgroups of Klein four-group V_4
  - E.g. {e, (1,2,3), (1,3,2)} is a subgroup of S_3
  - E.g. {0, 3}, {0, 2, 4} are subgroups of $(Z_6, \oplus)$
- For an element a in a group G, if the set $\langle a \rangle = \{a^n : n \in Z\}$ that consists all the integer power of a is a subset of G, then we call $\langle a \rangle$ a cyclic subgroup of G generated by a.
  - E.g. $\langle 4 \rangle = \{0, 2, 4\}$ is a cyclic subgroup of $(Z_6, \oplus)$
  - E.g. $\langle a \rangle = \{e, a\}$ is a cyclic subgroup of Klein four-group V_4
- A group G that can be generated by a finite set is said to be finitely generated.
  - E.g. Klein four-group V_4 can be generated by any of these two-element sets: {a, b}, {a, c}, or {b, c}

- Langrange's theorem: a group's order is dividable by the its subgroups' order.
  - E.g. group V_4 has order 4, and all of its subgroups: {e}, {e, a}, {e, b}, {e, c}, V_4 itself have order 1, 2, 4, which all divide 4;
  - E.g. $(Z_6, \oplus)$ has order 6, all subgroups: {0}, {0, 3}, {0, 2, 4}, and $(Z_6, \oplus)$ itself have order 1, 2, 3, 6, which all divide 6;
  - E.g. S_3 has order 6, all subgroups: {e}, {e, (1,2)}, {e, (1,3)}, {e, (2,3)}, {e, (1,2,3), (1,3,2)}, S_3 itself have order 1,2,3,6 dividing 6.
- Theorem of existence: a finite Abelian group with order n has at least one subgroup for each (positive) divisor of n.
- Theorem of unique: a finite cyclic group with order n has exact one subgroup for each divisor of n.
- Cauchy's theorem: a finite group with order n has at least one subgroup of order p, which is a prime that divides n.
- Sylow's first theorem: for a finite group with order $n=p^k m$, where p is a prime that does not divide m, it has at least one subgroup of order p^i for every integer i from 0 to k.

Isomorphism

- Two groups are isomorphism (G1 ≅ G2) if they are structurally identical: there exists a full bijective mapping between G_1 and G_2 which maintains the operations.
  - E.g. $(Z_4, \oplus)$, $(Z^*_5, \otimes)$, and V_4 are nonisomorphic for each pair;
  - E.g. $(Z_6, \oplus)$ and S_3 are nonisomorphic
  - E.g. U_3 and $(Z_3, \oplus)$ are isomorphic
  - E.g. V4 is isomorphic to M, which is a subgroup of $(M_2(Z), \times)$ that is consists of four matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$-A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{and} \quad -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

×	I	A	$-A$	$-I$
I	I	A	$-A$	$-I$
A	A	I	$-I$	$-A$
$-A$	$-A$	$-I$	I	A
$-I$	$-I$	$-A$	A	I

Classification of finite Abelian groups

- For two groups $(G_1, *_1)$ and $(G_2, *_2)$, the direct product of them $(G_1 \times G_2, *)$ is also a group, where:

$$G_1 \times G_2 = \{(a, b): a \in G_1, b \in G_2\}$$

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$$

- If G_1 and G_2 are finite groups, and their orders are m and n, then $G_1 \times G_2$ has order mn.
- If G_1 and G_2 are both Abelian, then the resulting (Abelian) group is called the direct sum of G_1 and G_2, written as $G_1 \oplus G_2$.
- Theorem: if gcd(m,n)=1, then $Z_m \oplus Z_n$ is cyclic and isomorphic to Z_{mn}.
  - E.g. $Z_2 \oplus Z_4$ is not cyclic, but $Z_2 \oplus Z_3$ is cyclic and $Z_2 \oplus Z_3 \cong Z_6$
- Generalized theorem: $Z_{m1} \oplus Z_{m2} \oplus \ldots \oplus Z_{mk}$ is cyclic if and only if $\gcd(m_i, m_j)=1$ for every distinct pair m_i and m_j, and $Z_{m1} \oplus Z_{m2} \oplus \ldots \oplus Z_{mk} \cong Z_{m1m2\ldots mk}$

Every finite Abelian group G is isomorphic to a direct sum of the form

$$\mathbf{Z}_{(p_1)^{k_1}} \oplus \mathbf{Z}_{(p_2)^{k_2}} \oplus \cdots \oplus \mathbf{Z}_{(p_r)^{k_r}}$$

where the p_i are (not necessarily distinct) primes and the k_i are (not necessarily distinct) positive integers. The collection of prime powers, $(p_i)^{k_i}$, for a given representation of G, are known as the **elementary divisors** of G.

Every finite Abelian group G is isomorphic to a direct sum of the form

$$\mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus \cdots \oplus \mathbf{Z}_{m_t}$$

where $m_1 \geq 2$, m_1 divides m_2, m_2 divides m_3, . . . , and m_{t-1} divides m_t. The integers m_1 through m_t are not necessarily distinct, but the list $m_1, \ldots, m_t$ is unique, and these integers are called the **invariant factors** of G.

Example 6.7 How many structurally distinct (that is, mutually nonisomorphic) Abelian groups are there of order 600?

Solution: Our first step is to find the prime factorization of 600:

$$600 = 2^3 \cdot 3 \cdot 5^2$$

Therefore, if G is an Abelian group of order 600, there are six possible collections of elementary divisors:

1) $2, 2, 2, 3, 5, 5$
2) $2, 2, 2, 3, 5^2$
3) $2, 2^2, 3, 5, 5$
4) $2, 2^2, 3, 5^2$
5) $2^3, 3, 5, 5$
6) $2^3, 3, 5^2$

Each of these lists of elementary divisors gives rise to an Abelian group, as follows:

1) $2, 2, 2, 3, 5, 5 \rightarrow \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_5$
2) $2, 2, 2, 3, 5^2 \rightarrow \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_{25}$
3) $2, 2^2, 3, 5, 5 \rightarrow \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_5$
4) $2, 2^2, 3, 5^2 \rightarrow \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_{25}$
5) $2^3, 3, 5, 5 \rightarrow \mathbf{Z}_8 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_5$
6) $2^3, 3, 5^2 \rightarrow \mathbf{Z}_8 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_{25}$

Therefore, there are six different Abelian groups (up to isomorphism) of order 600.
We can also figure out the invariant factors of each of these six groups. In each case, we must express the group in the form $\mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus \cdots \oplus \mathbf{Z}_{m_t}$, where $m_1 \geq 2$ and m_i divides m_{i+1}.

$2, 2, 3, 5, 5 \rightarrow$

2	2	2
		3
	5	5
↓	↓	↓

$$Z_2 \oplus Z_{10} \oplus Z_{30}$$

$2, 2, 2, 3, 5^2 \rightarrow$

2	2	2
		3
		5^2
↓	↓	↓

$$Z_2 \oplus Z_2 \oplus Z_{150}$$

$2, 2^2, 3, 5, 5 \rightarrow$

2	2^2
	3
5	5
↓	↓

$$Z_{10} \oplus Z_{60}$$

$2, 2^2, 3, 5^2 \rightarrow$

2	2^2
	3
	5^2
↓	↓

$$Z_2 \oplus Z_{300}$$

$2^3, 3, 5, 5 \rightarrow$

2^3	
3	
5	5
↓	↓

$$Z_5 \oplus Z_{120}$$

$2^3, 3, 5^2 \rightarrow$

2^3
3
5^2
↓

$$Z_{600}$$

Therefore, the six mutually nonisomorphic Abelian groups of order 600 can be expressed as follows, where in each case, we've written the representation of G in terms of the elementary divisors on the left, and the corresponding representation in terms of the invariant factors on the right:

1) $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_5 \cong \mathbf{Z}_2 \oplus \mathbf{Z}_{10} \oplus \mathbf{Z}_{30}$

2) $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_{25} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{150}$

3) $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_5 \cong \mathbf{Z}_{10} \oplus \mathbf{Z}_{60}$

4) $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_{25} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_{300}$

5) $\mathbf{Z}_8 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_5 \cong \mathbf{Z}_5 \oplus \mathbf{Z}_{120}$

6) $\mathbf{Z}_8 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_{25} \cong \mathbf{Z}_{600}$

Homomorphism

- Let (G, •) and (G', *) being groups, a function ϕ: G→G' with the property that

$$\phi(x \bullet y) = \phi(x) * \phi(y)$$

- For all the elements x and y in G, is called a group homomorphism.
- Monomorphism: one-to-one (injective) mapping
- Epimorphism: onto (surjective) mapping
- Isomorphism: one-to-one and onto (bijective) mapping
- Endomorphism: a homomorphism from a group to itself
- Automorphism: an isomorphism from a group to itself
- https://en.wikipedia.org/wiki/Bijection,_injection_and_surjection

1. If e is the identity in G, then $\phi(e)$ is the identity in G'.
2. If $g \in G$ has finite order m, then $\phi(g) \in G'$ also has order m.
3. If a^{-1} is the inverse of a in G, then $\phi(a^{-1})$ is the inverse of $\phi(a)$ in G'.
4. If H is a subgroup of G, then $\phi(H)$ is a subgroup of G', where:

$$\phi(H) = \{\phi(h): h \in H\}$$

5. If G is finite, then the order of $\phi(G)$ divides the order of G; if G' is finite, then the order of $\phi(G)$ also divides the order of G'.
6. If H' is a subgroup of G', then $\phi^{-1}(H')$ is a subgroup of G, where

$$\phi^{-1}(H') = \{h \in G: \phi(h) \in H'\}$$

If $\phi: G \to G'$ is a homomorphism of groups, then $\{e'\}$, where e' is the identity in G', is a subgroup—the trivial subgroup—of G'. By property 6, the inverse image of $\{e'\}$ is a subgroup of G. This subgroup is given a name: It's called the **kernel** of ϕ, denoted by $\ker\phi$:

$$\ker\phi = \{g \in G: \phi(g) = e'\}$$

A homomorphism is a monomorphism if and only if its kernel is trivial.

Example 6.9 Let U_n be the multiplicative group of the n^{th} roots of unity; this group is cyclic of order n and is generated by $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. If we define ϕ: $(\mathbf{Z}, +) \to U_n$ by the equation $\phi(a) = \omega^a$, show that ϕ is a homomorphism. Is ϕ a monomorphism? an epimorphism? an isomorphism?

Solution: The function ϕ is a homomorphism, since:

$$\phi(a+b) = \omega^{a+b} = \omega^a\omega^b = \phi(a)\phi(b)$$

The kernel of this homomorphism is the subgroup:

$$\ker\phi = \{a \in \mathbf{Z}: \omega^a = 1\} = \{mn: m \in \mathbf{Z}\}$$

The function ϕ is an epimorphism, but not a monomorphism (and thus not an isomorphism), since it's not one-to-one (its kernel is not trivial). We also know that ϕ is not an isomorphism, because an infinite group cannot be isomorphic to a finite group.

Example 6.10 Let $GL(n, \mathbf{R})$ be the multiplicative group of invertible n by n matrices with real entries. Show that the function $\phi: GL(n, \mathbf{R}) \to (\mathbf{R}^*, \times)$, given by $\phi(A) = \det A$, is a homomorphism, and find $\ker\phi$.

Solution: The function ϕ is a homomorphism because:

$$\phi(AB) = \det(AB) = (\det A)(\det B) = \phi(A)\phi(B)$$

The kernel of this homomorphism is the subgroup:

$$\ker\phi = \{A \in GL(n, \mathbf{R}): \det A = 1\} = SL(n, \mathbf{R})$$

Example 6.12 Is there a nontrivial homomorphism ϕ: $(Z_8, +) \rightarrow (Z_3, +)$?

Solution: If the answer is *yes*, then the homomorphic image of Z_8 must be a subgroup of Z_3. Since ϕ is nontrivial, the order of $\phi(Z_8)$ is not 1. By Lagrange's theorem, then, the order of $\phi(Z_8)$ must be 3. However, according to property 5 listed above, the order of $\phi(Z_8)$ must divide the order of Z_8. This is a contradiction, since 3 does not divide 8. Therefore, the answer to the question is *no*.

Example 6.14 Let $\phi: G \to G$ be a function such that $\phi(g) = g^{-1}$ for every g in G. Show that G is Abelian if and only if ϕ is an endomorphism.

Solution: First, let's assume that G is Abelian. Since the inverse of xy is $y^{-1}x^{-1}$ in any group (Abelian or not), we know that $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1}$. Now, because G is Abelian, $y^{-1}x^{-1} = x^{-1}y^{-1}$, which is equal to $\phi(x)\phi(y)$. Since $\phi(xy) = \phi(x)\phi(y)$, ϕ is a homomorphism of G to itself.

To complete the solution, let's now assume that ϕ is a homomorphism. Then $\phi(xy) = \phi(x)\phi(y)$, so $(xy)^{-1} = x^{-1}y^{-1}$, which implies $y^{-1}x^{-1} = x^{-1}y^{-1}$. Taking the inverse of both sides of this last equation, we get $(y^{-1}x^{-1})^{-1} = (x^{-1}y^{-1})^{-1}$, which is equivalent to $xy = yx$. This shows that G is Abelian.

Example 6.15 Is the group $(\mathbf{R}, +)$ isomorphic to the group $(\mathbf{R}^+, \times)$?

Solution: Define a function $\phi: (\mathbf{R}, +) \to (\mathbf{R}^+, \times)$ by the equation $\phi(x) = e^x$, where now e denotes the base of the natural logarithm. We'll show that ϕ is an isomorphism. First,

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

so ϕ is a homomorphism. Next,

$$\phi(x) = 1 \quad \Rightarrow \quad e^x = 1 \quad \Rightarrow \quad x = 0 \quad \Rightarrow \quad \ker\phi = \{0\}$$

which shows that ϕ is one-to-one. Finally, for every x in $\mathbf{R}^+$, we have

$$\phi(\log x) = e^{\log x} = x$$

so ϕ is onto. Since ϕ is an isomorphism, we have $(\mathbf{R}, +) \cong (\mathbf{R}^+, \times)$.

Equivalence relation and equivalence class

- A given binary relation ~ on a set X is said to be an equivalence relation if and only if it is reflexive, symmetric and transitive. That is, for all a, b and c in X:
  - a ~ a. (Reflexivity)
  - a ~ b if and only if b ~ a. (Symmetry)
  - if a ~ b and b ~ c then a ~ c. (Transitivity)
- X together with the relation ~ is called a setoid. The equivalence class of a under ~, denoted [a], is defined as $[a]=\{b: b\sim a, b\in X\}$
- Examples:
  - Let the set {a,b,c} have the equivalence relation
    {(a,a), (b,b), (c,c), (b,c), (c,b)}.
  - All the equivalence classes : [a]={a}, [b]=[c]={b,c}
  - Under this equivalence relation, there exist an unique partition of X: { {a}, {b,c} }.

- The following are all equivalence relations:
  - "Has the same birthday as" on the set of all people.
  - "Is similar to" on the set of all triangles.
  - "Is congruent to" on the set of all triangles.
  - "Is congruent to, modulo n" on the integers.
  - "Has the same image under a function" on the elements of the domain of the function.
  - "Has the same absolute value" on the set of real numbers
  - "Has the same cosine" on the set of all angles.
- Some relations that are not equivalence
  - E.g. The relation "≥" between real numbers is reflexive and transitive, but not symmetric. For example, $7 \geq 5$ does not imply that $5 \geq 7$.

Quotient set

- Given a set S and an equivalence relation ~ on S, all the equivalence classes form a partition of S (i.e. a set of set), which is also called quotient set or the quotient space of S by ~ and is denoted by S / ~.
- Every two equivalence classes are either equal or disjoint.
- Examples:
  - Let $X = R^2$ be the standard Cartesian plane, and let Y be a line through the origin in X. Then the quotient space X/Y can be identified with the space of all lines in X which are parallel to Y. That is to say that, the elements of the set X/Y are lines in X parallel to Y. This gives one way in which to visualize quotient spaces geometrically.
  - Another example is the quotient of R^n by the subspace spanned by the first m standard basis vectors. Two vectors of R^n are in the same congruence class modulo the subspace if and only if they are identical in the last n−m coordinates. The quotient space R^n/ R^m is isomorphic to R^{n-m}.
  - More generally, if V is an (internal) direct sum of subspaces U and W: $V=U\oplus W$, then the quotient space V/U is isomorphic to W.

Conjugate

- Let G be a group. Two elements a and b of G are conjugate, if there exists an element g in G such that $gag^{-1} = b$ (or $ga = bg$).
  - If b is a conjugate of a, then a is also a conjugate of b. (proof: $b = gag^{-1}$, $a = g^{-1}bg$)
  - Every element is conjugate to itself. (proof: $aa^{-1} = a^{-1}a = e$)
  - If a is a conjugate of b, and b is a conjugate of c, then a is also a conjugate of c. (proof: $b = x^{-1}ax$, $c = y^{-1}by$, so $c = (xy)^{-1}a(xy)$)
  - So an element can have multiple conjugates. We can put all of them together as a set, which is named the conjugacy class of a. Therefore conjugation results in a partition of a group.
- In the case of the group GL(n) of invertible matrices, the conjugacy relation is called matrix similarity.

Conjugacy class

- Let G be a group and a is an element, the set that is consisted by all the conjugates of a is called the conjugacy class of a, denoted as Cl(a) = { b $\in$ G | there exists g $\in$ G with b = gag^{-1} }
  - Cl(e)= {e}
  - If G is Abelian, then gag^{-1} = a for all a and g in G; so Cl(a) = {a} for all a in G.
- Examples
  - Symmetric group S_3 has three conjugacy classes: {e}, {(1,2), (1,3), (2,3)}, {(1,2,3), (1,3,2)}
  - S_4 has five conjugacy classes: {e}, (2), (3), (4), (2)(2)

$b \cdot a \cdot b^{-1}$	0	1	2	4	3	5	6	7	12	18	13	19	8	10	14	20	16	22	9	11	15	21	17	23
$b^{-1} \cdot a \cdot b$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
1	1	5	5	2	2	1	1	21	21	14	14	5	5	21	21	6	6	2	2	14	14	6	6
2	5	2	1	5	1	14	21	14	1	21	1	6	21	6	5	21	5	6	14	6	2	14	2
3	4	4	3	3	4	15	20	20	15	15	20	11	19	19	11	11	19	8	12	12	8	8	12
4	3	3	4	4	3	20	15	15	20	20	15	19	11	11	19	19	11	12	8	8	12	12	8
5	2	1	2	1	5	21	14	1	14	1	21	21	6	5	6	5	21	14	6	2	6	2	14
6	6	14	14	21	21	6	6	2	2	5	5	14	14	2	2	1	1	21	21	5	5	1	1
7	7	16	16	23	23	7	7	23	23	16	16	16	16	23	23	7	7	23	23	16	16	7	7
8	11	12	15	19	20	12	19	8	3	11	4	8	20	12	4	15	3	11	15	19	3	20	4
9	10	17	13	22	18	13	18	22	9	17	10	10	22	18	17	9	13	9	17	13	22	10	18
10	9	13	17	18	22	18	13	9	22	10	17	22	10	17	18	13	9	17	9	22	13	18	10
11	8	15	12	20	19	19	12	3	8	4	11	20	8	4	12	3	15	15	11	3	19	4	20
12	19	8	20	11	15	8	11	12	4	19	3	12	15	8	3	20	4	19	20	11	4	15	3
13	18	10	22	9	17	9	10	18	17	13	22	17	13	22	9	10	18	22	18	17	10	9	13
14	21	6	21	6	14	2	5	6	5	6	2	2	1	14	1	14	2	5	1	21	1	21	5
15	20	11	19	8	12	3	4	19	11	12	8	4	3	20	15	8	12	3	4	15	20	11	19
16	23	7	23	7	16	23	16	7	16	7	23	23	7	16	7	16	23	16	7	23	7	23	16
17	22	9	18	10	13	22	17	13	10	18	9	18	9	10	13	22	17	13	10	9	18	17	22
18	13	22	10	17	9	10	9	17	18	22	13	13	17	9	22	18	10	18	22	10	17	13	9
19	12	20	8	15	11	11	8	4	12	3	19	15	12	3	8	4	20	20	19	4	11	3	15
20	15	19	11	12	8	4	3	11	19	8	12	3	4	15	20	12	8	4	3	20	15	19	11
21	14	21	6	14	6	5	2	5	6	2	6	1	2	1	14	2	14	1	5	1	21	5	21
22	17	18	9	13	10	17	22	10	13	9	18	9	18	13	10	17	22	10	13	18	9	22	17
23	16	23	7	16	7	16	23	16	7	23	7	7	23	7	16	23	16	7	16	7	23	16	23

Normal subgroup

- A normal subgroup (or called invariant subgroup) is a subgroup which is invariant under conjugation by members of the group of which it is a part.
- In other words, a subgroup H of a group G is normal in G if and only if gH = Hg for all g in G;
  - i.e., the sets of left coset and right coset of any g∈G coincide (gH = Hg);
- Normal subgroups (and only normal subgroups) can be used to construct quotient groups from a given group;
- Évariste Galois was the first to realize the importance of the existence of normal subgroups.

A subgroup, N, of a group, G, is called a **normal subgroup** if it is invariant under conjugation; that is, the conjugation of an element of N by an element of G is still in N:[3]

$$N \triangleleft G \Leftrightarrow \forall\, n \in N,\ \forall\, g \in G:\ gng^{-1} \in N.$$

- The image of conjugation of N by any element of G is N: $\forall g \in G, gNg^{-1} = N$.
- Any two elements commute regarding the normal subgroup membership relation: $\forall g, h \in G, gh \in N \Leftrightarrow hg \in N$.
- The subgroup {e} consisting of just the identity element of G and G itself are always normal subgroups of G. The former is called the trivial subgroup, and if these are the only normal subgroups, then G is said to be simple.
- All subgroups, N, of an abelian group, G, are normal, because gN = Ng. A group that is not abelian but for which every subgroup is normal is called a Hamiltonian group.
- The translation group in any dimension is a normal subgroup of the Euclidean group (with the orthogonal group as the quotient group); for example in 3D rotating, translating, and rotating back results in only translation
- The largest subgroup of H that is normal in G is called the core of H in G.
- Examples:
  - S3 has four non-trivial subgroups: {e, (1,2)}, {e, (1,3)}, {e, (2,3)}, {e, (1,2,3), (1,3,2)}, but only the last one is a normal subgroup.

Coset

- if G is a group, and H is a subgroup of G, and g is an element of G, then

  $gH = \{ gh : h \in H \}$ is the left coset of H in G with respect to g

  $Hg = \{ hg : h \in H \}$ is the right coset of H in G with respect to g.
- Although derived from a subgroup, cosets are not usually themselves subgroups of G, only subsets.
- In other words, if a subgroup H is the same as its conjugate subgroup gHg^{-1}, then H is called normal.
- The cosets form a group called the quotient group or factor group.
- Examples
  - Z_8 has two non-trivial subgroups: {0, 4}, {0,2,4,6}. Left cosets of {0,4} are {0,4}, {1,5}, {2,6}, {3,7}; left cosets of {0,2,4,6} are {0,2,4,6}, {1,3,5,7}. Both of {0,4} and {0,2,4,6} are normal subgroups

Quotient group

- Let N be a normal subgroup of a group G. We define the set G/N to be the set of all left cosets of N in G, i.e., G/N = { aN : a ∈ G }, then the set G/N together with the multiplication operation on sets (i.e. subsets in G) forms a group, called quotient group.
- The key: if N is a normal subgroup, the multiplication of its left cosets satisfies closure, associativity, identity, inversibility (homomorphism)
  - Closure: (aN)(bN) = a(Nb)N = a(bN)N = (ab)NN = (ab)N
  - Identity and inversibility: $(a^{-1}N)(aN) = a^{-1}aN = N$
- The importance: the study of group G is reduced to that of its normal group N and quotient group G/N.
- Notice: they are not ordered sets
- Example
  - Consider the group with addition modulo 6: G = {0, 1, 2, 3, 4, 5}.
  - Consider the subgroup N = {0, 3}, which is normal because G is Abelian. Then the set of (left) cosets is of size three:

G/N = { a+N : a ∈ G } = { {0, 3}, {1, 4}, {2, 5} } = { 0+N, 1+N, 2+N }

  - Consider another subgroup N = {0, 2, 4}, the quotient group becomes:

G/N = { {0, 2, 4}, {1, 3, 5} } = { 0+N, 1+N }

Center

- In abstract algebra, the center of a group, G, is the set of elements that commute with every element of G. It is denoted Z(G), from German Zentrum, meaning center. In set-builder notation,

$$Z(G) = \{z \in G \mid \forall g \in G, zg = gz\} .$$

- The center is always a normal subgroup, $Z(G) \triangleleft G$. As a subgroup, it is always characteristic, but is not necessarily fully characteristic. The quotient group, G / Z(G), is isomorphic to the inner automorphism group, Inn(G).
- A group G is abelian if and only if Z(G) = G. At the other extreme, a group is said to be centerless if Z(G) is trivial; i.e., consists only of the identity element.
- The elements of the center are sometimes called central.

Example 6.16 A subgroup N of G is said to be a **normal** subgroup if $xnx^{-1} \in N$ for every n in N and every x in G. If $\phi: G \to G'$ is a homomorphism of groups, show that $\ker\phi$ is a *normal* subgroup of G.

Solution: We already know that $\ker\phi$ is a subgroup of G; we're asked to show that it's actually a normal subgroup. Let g be any element in $\ker\phi$. Since $\phi(g) = e'$ and $\phi(x^{-1}) = [\phi(x)]^{-1}$, the following is true for every x in G:

$$\phi(xgx^{-1}) = \phi(x) \cdot \phi(g) \cdot \phi(x^{-1}) = \phi(x) \cdot e' \cdot \phi(x^{-1}) = \phi(x) \cdot [\phi(x)]^{-1} = e'$$

Therefore, $xgx^{-1} \in \ker\phi$. Since we've shown that $xgx^{-1} \in \ker\phi$ for every g in $\ker\phi$ and every x in G, we conclude that $\ker\phi$ is, by definition, a normal subgroup of G.

Example 6.18 Let G be a group. For a fixed element a in G, define a function $\phi_a: G \to G$ by the equation $\phi_a(g) = aga^{-1}$.

(a) Show that ϕ_a is an automorphism. (It's called the **inner automorphism induced by a**.)

(b) Let Aut(G) denote the collection of all automorphisms of G. According to the operation of function composition, (Aut(G), $\circ$) is a group. Show that the set of all inner automorphisms of G, Inn(G) = $\{\phi_a: a \in G\}$, is a subgroup of Aut(G).

(c) Describe Inn(G) if G is Abelian.

Solution:

(a) First, the following equation establishes that ϕ_a is a homomorphism:

$$\phi_a(g_1g_2) = ag_1g_2a^{-1} = ag_1eg_2a^{-1} = ag_1a^{-1}ag_2a^{-1} = (ag_1a^{-1})(ag_2a^{-1}) = \phi_a(g_1)\phi_a(g_2)$$

Next, we'll prove that ϕ_a is one-to-one. We can do this in two ways; we can either notice that

$$\phi_a(g_1) = \phi_a(g_2) \Rightarrow ag_1a^{-1} = ag_2a^{-1} \Rightarrow a^{-1}(ag_1a^{-1})a = a^{-1}(ag_2a^{-1})a \Rightarrow g_1 = g_2$$

or we can show that $\ker\phi_a = \{e\}$:

$$g \in \ker\phi_a \Leftrightarrow \phi_a(g) = e \Leftrightarrow aga^{-1} = e \Leftrightarrow ag = ea \Leftrightarrow g = e$$

Finally, we need to show that ϕ_a is onto G. Since G is a group, we know that $a^{-1}ga \in G$ for every a and g in G. Now, for every g in G, notice that the image of $a^{-1}ga$ is g:

$$\phi_a(a^{-1}ga) = a(a^{-1}ga)a^{-1} = (aa^{-1})g(aa^{-1}) = ege = g$$

Therefore, ϕ_a is onto, so we're able to conclude that it's an isomorphism of G to itself; that is, it's an automorphism of G.

(b) To show that Inn(G) is a subgroup of Aut(G), we need to show that Inn(G) is closed under the group operation, it contains the identity, and it contains the inverse of every element in Inn(G). Let's first establish closure. Let ϕ_a and ϕ_b be elements of Inn(G) then, since

$$\begin{aligned}(\phi_a \circ \phi_b)(g) = \phi_a(\phi_b(g)) = \phi_a(bgb^{-1}) &= a(bgb^{-1})a^{-1} \\ &= (ab)g(b^{-1}a^{-1}) \\ &= (ab)g(ab)^{-1} \\ &= \phi_{ab}(g)\end{aligned}$$

is true for every g in G, we know that $\phi_a \circ \phi_b = \phi_{ab}$ so Inn(G) is closed under function composition. Next, the identity of Aut(G) is clearly the identity map, id: $G \to G$, where id(g) = g for all g in G. But if e is the identity of G, then the inner automorphism induced by e, ϕ_e, *is* the identity map, because

$$\phi_e(g) = ege^{-1} = ege = g$$

for every g in G. Therefore, Inn(G) contains the identity. Finally, we'll show that if a^{-1} is the inverse of a, then the map $\phi_{a^{-1}}$ is the inverse of ϕ_a. The calculation

$$aga^{-1} = g' \quad \Leftrightarrow \quad ga^{-1} = a^{-1}g' \quad \Leftrightarrow \quad g = a^{-1}g'a \quad \Leftrightarrow \quad g = a^{-1}g'(a^{-1})^{-1}$$

means that $\phi_a(g) = g' \Leftrightarrow g = \phi_{a^{-1}}(g')$, so $\phi_{a^{-1}}$ is indeed the inverse of ϕ_a. Thus, Inn(G) ≤ Aut(G).

(c) If G is Abelian, then for any a in G, $\phi_a(g) = aga^{-1} = aa^{-1}g = g$ for every g in G; so, for every a in G, the inner automorphism ϕ_a is just the identity map. Therefore, if G is Abelian, Inn(G) is the trivial subgroup of Aut(G).

Rings

- A ring is a special binary structure with two binary operations
- A set R with two binary operations (+ and •) is called a ring if the following conditions are satisfied:
  - (R, +) is an Abelian group
  - (R, •) is a semigroup (associativity)
  - Distributive law: for any a,b,c in R, we have

    $a \bullet (b+c) = a \bullet b + a \bullet c$ $\qquad$ $(a+b) \bullet c = a \bullet c + b \bullet c$
- A ring with unity: (R, •) is a monoid
- Commutative ring: the multiplication is commutative
- Subring: S is a subset of R and forms a ring (S, +, •)

1. $(\mathbf{Z}, +, \bullet)$ is the simplest example of a ring; it's a commutative ring with unity, called the **ring of integers**. We mentioned earlier that $(\mathbf{Z}, \bullet)$ is not a group because most elements have no inverse; however, the definition of a ring doesn't require that $(R, \bullet)$ be a group, only a semigroup. If n is a positive integer and we let $n\mathbf{Z} = \{nk: k \in \mathbf{Z}\}$, then $(n\mathbf{Z}, +, \bullet)$ is a subring of $\mathbf{Z}$. Notice that, if $n > 1$, then $n\mathbf{Z}$ is also a commutative ring, but not a ring with unity.

2. The ring of integers is a subring of the rings $(\mathbf{Q}, +, \bullet)$, $(\mathbf{R}, +, \bullet)$, and $(\mathbf{C}, +, \bullet)$.

3. Since $(\mathbf{Z}_n, +)$ is an Abelian group and $(\mathbf{Z}_n, \bullet)$ is a semigroup, $(\mathbf{Z}_n, +, \bullet)$ is the **ring of integers modulo** n.

4. The set of n by n matrices with entries in $\mathbf{R}$, with the operations of matrix addition and multiplication, $(M_n(\mathbf{R}), +, \times)$, is a ring with unity, a noncommutative ring if $n > 1$. $M_n(\mathbf{Q})$ and $M_n(\mathbf{Z})$ are subrings.

5. The set $R = \left\{a + b\sqrt{2}: a, b \in \mathbf{Z}\right\}$, together with the usual operations of addition and multiplication, is a commutative ring with unity. It's straightforward to check that R is closed under both addition and multiplication, since:

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

and

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$$

Notice, however, that the set $C = \left\{a + b\sqrt[3]{2}: a, b \in \mathbf{Z}\right\}$ does not form a ring, since it's not closed under multiplication:

$$(a_1 + b_1\sqrt[3]{2})(a_2 + b_2\sqrt[3]{2}) = (a_1a_2) + (a_1b_2 + a_2b_1)\sqrt[3]{2} + b_1b_2\sqrt[3]{4} \notin C$$

6. With the operations of addition and multiplication in **C**, the set

$$\mathbf{Z}[i] = \left\{ a + bi \colon a,\ b \in \mathbf{Z} \text{ and } i = \sqrt{-1} \right\}$$

is a subring of **C**, called the **ring of Gaussian integers**.

7. Let R be a ring, and consider the collection of all polynomials—including the zero polynomial—in the variable (or **indeterminate**) x with coefficients in R:

$$R[x] = \left\{ r_0 + r_1 x + r_2 x^2 + \cdots + r_n x^n : r_i \in R \right\}$$

Then $R[x]$ is also a ring, called the **ring of polynomials in x over R**.

8. The collection of all functions $f\colon \mathbf{R} \to \mathbf{R}$ is denoted $\mathbf{R}^{\mathbf{R}}$. With the operations of addition—where $(f + g)(x) = f(x) + g(x)$—and pointwise multiplication—where $(fg)(x) = f(x)g(x)$—$\mathbf{R}^{\mathbf{R}}$ becomes a commutative ring with unity, called the **ring of real-valued functions on R**. The additive identity is the constant function 0, and the multiplicative identity is the constant function 1.

Ring homomorphism

- Let (R, +, ×), (R', $\oplus$, $\otimes$) be rings, a function ϕ: R→R' is called a ring homomorphism if both of the following conditions hold for every a and b in R:

$$\phi(a+b) = \phi(a) \oplus \phi(b)$$

$$\phi(a \times b) = \phi(a) \otimes \phi(b)$$

1. The **kernel** of a ring homomorphism is the set $\ker \phi = \{a \in R: \phi(a) = 0'\}$, where $0'$ is the additive identity in R'. Just as the kernel of a group homomorphism $\phi: G \to G'$ is always a subgroup of G, the kernel of a ring homomorphism $\phi: R \to R'$ is always a subring of R.
2. The image of R, $\phi(R) = \{\phi(r): r \in R\}$, is a subring of R'.
3. The image of 0, the additive identity in R, must be $0'$, the additive identity in R'. It follows from this that $\phi(-r) = -\phi(r)$ for every r in R, where $-r$ is the additive inverse of r.

- Examples
  - The function ϕ: $Z \rightarrow Z_n$ given by $\phi(k)$ = the unique integer in Z_n that is congruent to k (mod n) is a ring homomorphism (actually, it is a ring epimorphism, because it is onto);

Let $(R, +, \times)$ and $(R', \oplus, \otimes)$ be rings. It's possible for $\phi: (R, +) \to (R', \oplus)$ to be a group homomorphism but not a ring homomorphism. Let $R = R' = \mathbf{Z}$, the ring of integers. Then the function $\phi: (\mathbf{Z}, +) \to (\mathbf{Z}, +)$ given by $\phi(m) = 2m$ is a group homomorphism, but ϕ does not preserve the operation of multiplication, since $\phi(mn) = 2mn$, but $\phi(m)\phi(n) = (2m)(2n) = 4mn$.

Let $(R, +, \times)$ and $(R', \oplus, \otimes)$ be rings. It's possible for $\phi: (R, \times) \to (R', \otimes)$ to be a group homomorphism but not a ring homomorphism. Let $R = GL(2, \mathbf{R})$, and let $R' = \mathbf{R}$; these are groups under matrix multiplication and ordinary multiplication, respectively. Then the function ϕ: $(R, \times) \to (\mathbf{R}, \bullet)$ given by $\phi(A) = \det A$ is a group homomorphism, but not a ring homomorphism since ϕ does not preserve the operation of addition: In general, $\det(A + B) \neq \det A + \det B$.

Example 6.22 Describe all the ring endomorphisms of $\mathbf{Z}$.

Solution: For any rings R and R', the **zero map**, z: $R \to R'$, given by $z(r) = 0'$ for every r in R, is always a ring homomorphism (although certainly not a very interesting one). So now let's assume that f: $\mathbf{Z} \to \mathbf{Z}$ is a *nonzero* ring endomorphism. Since 1 generates the cyclic group $\mathbf{Z}$, $\phi(1)$ cannot be equal to 0, because if it were, then $\phi(m)$ would equal 0 for every m in $\mathbf{Z}$ [because $\phi(m) = \phi(1 \bullet m) = \phi(1)\phi(m)$], contradicting our assumption that f is a nonzero map. Then $[\phi(1)]^2 = \phi(1)\phi(1) = \phi(1 \bullet 1) = \phi(1)$, but $\phi(1)$ is not equal to 0. The only nonzero integer n that satisfies $n^2 = n$ is $n = 1$, so we must have $\phi(1) = 1$. Now, if m is a positive integer, then $\phi(m) = \phi(1 + 1 + \ldots + 1)$, with m summands, which gives $\phi(m) = \phi(1) + \phi(1) + \ldots + \phi(1) = m\phi(1) = m \bullet 1 = m$; and $\phi(-m) = \phi(-1 + -1 + \ldots + -1)$, with m summands, which gives $\phi(-m) = \phi(-1) + \phi(-1) + \ldots + \phi(-1) = m(-\phi(1)) = -m$. And finally, if $m = 0$, then $\phi(0) = 0$, since any ring homomorphism maps the additive identity to the additive identity. Therefore, for every integer m, we have $\phi(m) = m$, so ϕ is the identity map. We conclude that there are only two ring homomorphisms from $\mathbf{Z}$ to itself: the zero homomorphism and the identity homomorphism.

Integral domain

- Integral domain: a commutative ring with unity (1≠0) that has no zero divisors.
  - E.g. In Z_6, we have 3*4=0, so Z_6 is not a integral domain
  - Cancellation law (a≠0 and ab=ac ➔ b=c) is only guaranteed in a integral domain

A nonzero element $m \in \mathbf{Z}_n$ is a zero divisor if and only if m and n are not relatively prime.

And this fact leads directly to the following important result:

If n is prime, then $\mathbf{Z}_n$ is an integral domain.

Fields

- A commutative division ring is called a field

Let a be a nonzero element of a ring R with unity. Since the multiplicative binary structure $(R, \bullet)$ isn't required to be a group, a may not have an inverse in R. However, if a *does* have a multiplicative inverse—that is, if it's **invertible**—then a is called a **unit**. (Don't confuse *unit* with *unity*: Unity is the unique multiplicative identity in R (a unit is a nonzero element with a multiplicative inverse.) For example, in the ring $\mathbf{Z}_6$, the element 5 is a unit since it has a multiplicative inverse (namely, itself, since $5 \bullet 5 = 1$ in $\mathbf{Z}_6$), but 2 is not a unit; there is no element b in $\mathbf{Z}_6$ such that $2 \bullet b = 1$. If every nonzero element in R is a unit—that is, if $(R^*, \bullet)$ is a group—then R is called a **division ring**. This name arises since in such a ring, every equation of the form $a \bullet x = c$ (with $a \neq 0$) can be solved for x by multiplying both sides by a^{-1}; that is, by "dividing by a." A commutative division ring is called a **field**. Let's look at some examples.

1. $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ are fields, but $\mathbf{Z}$ is not. $\mathbf{Z}$ is not a field since the only units in $\mathbf{Z}$ are 1 and –1.

2. The commutative ring with unity $\mathbf{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} : a, b \in \mathbf{Q}\right\}$ is a field. All we need to show is that every nonzero element in $\mathbf{Q}(\sqrt{2})$ has an inverse in $\mathbf{Q}(\sqrt{2})$; if a and b are not both zero, then:

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \bullet \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in \mathbf{Q}(\sqrt{2})$$

3. It's not difficult to show that a *finite* integral domain must be a field. Using this result, it follows that if p is a prime, then $\mathbf{Z}_p$ is a field (our first example of a *finite* field). In particular, this means that every nonzero element in $\mathbf{Z}_p$ is a unit; this would not be true if p weren't prime.

4. Consider the subset K of $M_2(\mathbf{R})$ that consists of the following 2 by 2 matrices:

$$K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbf{R} \right\}$$

This set contains the additive identity (the zero matrix)—by taking $a = b = 0$—and the multiplicative identity (the 2 by 2 identity matrix)—by taking $a = 1$ and $b = 0$. Since K is closed under addition,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in K$$

and multiplication,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \in K$$

it follows that K is a subring with unity of $M_2(\mathbf{R})$. But although matrix multiplication is generally not commutative, multiplication in K *is* commutative, since:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}=\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Now, if a and b are not both zero, we have

$$\det\begin{pmatrix} a & b \\ -b & a \end{pmatrix}=a^2+b^2\neq 0 \quad\Rightarrow\quad \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ is invertible}$$

which shows that every nonzero element of K is a unit. Therefore, this set of matrices is a commutative division ring—it's a field! In fact, it can be shown that K is structurally identical—isomorphic—to $\mathbf{C}$, the field of complex numbers.

- Kolmogorov probability theory
- Error correcting codes
- Klein four-group
- Rubik's Cube
- Symmetric group
- Symmetry group
- Erlangen program
- Galois Theory
- Lie group and Lie algebra

Applications

Kolmogorov probability theory

Definition 1.2.1 A collection of subsets of S is called a *sigma algebra* (or *Borel field*), denoted by $\mathcal{B}$, if it satisfies the following three properties:

a. $\emptyset \in \mathcal{B}$ (the empty set is an element of $\mathcal{B}$).

b. If $A \in \mathcal{B}$, then $A^c \in \mathcal{B}$ ($\mathcal{B}$ is closed under complementation).

c. If $A_1, A_2, \ldots \in \mathcal{B}$, then $\cup_{i=1}^{\infty} A_i \in \mathcal{B}$ ($\mathcal{B}$ is closed under countable unions).

Example 1.2.2 (Sigma algebra–I) If S is finite or countable, then these technicalities really do not arise, for we define for a given sample space S,

$$\mathcal{B} = \{\text{all subsets of } S, \text{ including } S \text{ itself}\}.$$

Example 1.2.3 (Sigma algebra–II) Let $S = (-\infty, \infty)$, the real line. Then $\mathcal{B}$ is chosen to contain all sets of the form

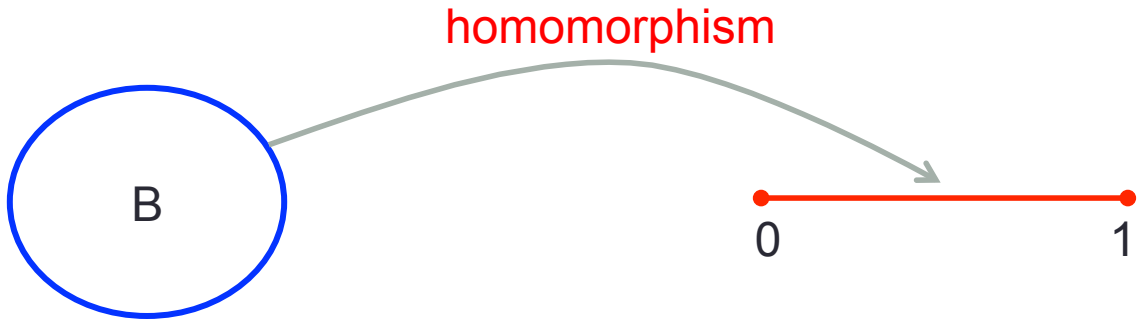
$$[a, b], \quad (a, b], \quad (a, b), \quad \text{and} \quad [a, b)$$

Definition 1.2.4 Given a sample space S and an associated sigma algebra $\mathcal{B}$, a *probability function* is a function P with domain $\mathcal{B}$ that satisfies

1. $P(A) \geq 0$ for all $A \in \mathcal{B}$.
2. $P(S) = 1$.
3. If $A_1, A_2, \ldots \in \mathcal{B}$ are pairwise disjoint, then $P(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i)$.

Theorem 1.2.8 *If P is a probability function and A is any set in $\mathcal{B}$, then*

a. $P(\emptyset) = 0$, *where $\emptyset$ is the empty set;*
b. $P(A) \leq 1$;
c. $P(A^c) = 1 - P(A)$.



Ordinary mapping

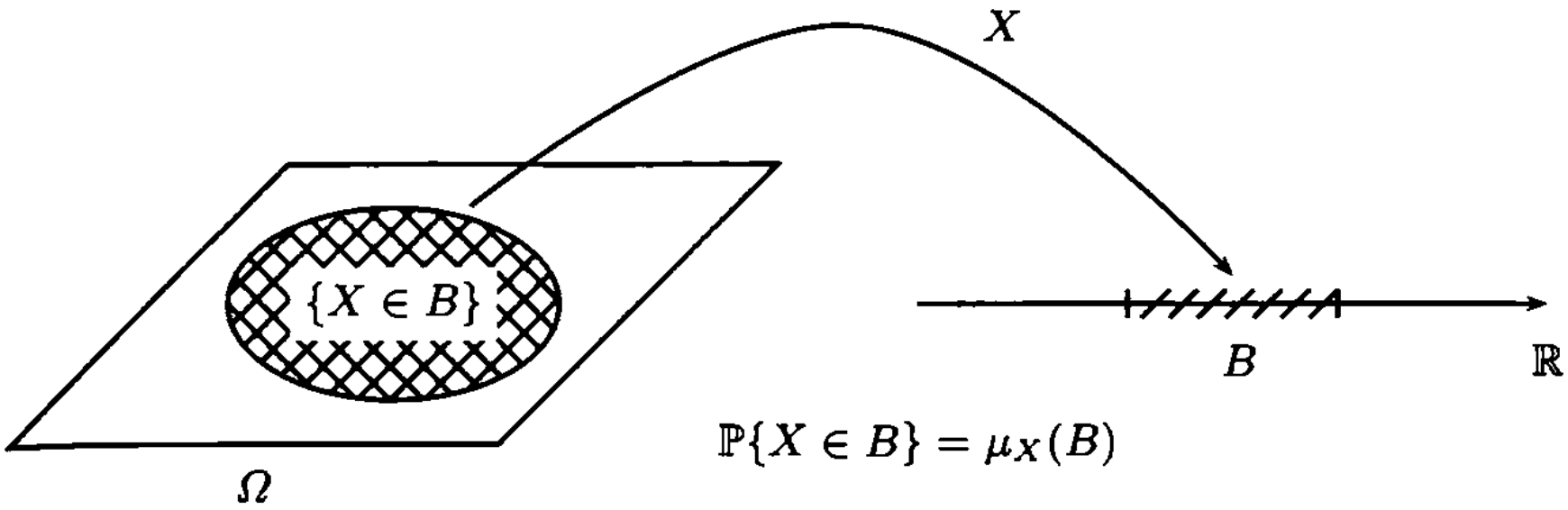


Fig. 1.2.1. Distribution measure of X.

Definition 1.2.3. *Let X be a random variable on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$. The* distribution measure of X *is the probability measure μ_X that assigns to each Borel subset B of $\mathbb{R}$ the mass $\mu_X(B) = \mathbb{P}\{X \in B\}$ (see Figure 1.2.1).*

Error correcting codes

- Problem: when information is transferred, some errors might be introduced due to the environmental noises, how to correct them when you receive the message?
- Idea: add more data to constrain the information in certain mathematical structures and the receiver is able to detect and recover it;
- GL(2): also F_2 or Z_2, is the Galois field of two elements. It is the smallest finite field.

Logical XOR

+	0	1
0	0	1
1	1	0

Logical AND

×	0	1
0	0	0
1	0	1

- Let's consider an example of transferring a message X with 15 bits, i.e. $x_i \in F_2$, i=1,2,…,15.
- Construct linear equations on F_2: HX = 0

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}_{4\times 15}$$

- The message is an element in the set of the general solutions of this linear system.
- Now, suppose there is an error at the i^{th} bit in X (either 0 to 1 or 1 to 0), that is $Y = X + e_i$, then $HY = HX + He_i = He_i$.
- If we carefully design H to make He_i having 15 distinct values corresponding to the e_i, then we can detect the error index i given He_i, and correct it by: $X = Y + e_i$.

- Consider a message $X = (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)^T$, it is easy to prove that $HX=0$;
- Add an error on 6^{th} bit: $Y = (1,1,1,1,1,0,1,1,1,1,1,1,1,1,1)^T$;
- Then, $HY = (0,1,1,0)^T$, so the error is at the 6^{th} bit, the correction is: $X = Y + (0,0,0,0,0,1,0,0,0,0,0,0,0,0,0)^T$
- The rank of H is 4, but with 15 variables, so the solution set (space) is an 11 dimensional space on F_2 with 2^{11} elements. In other words, there are only 11 free variables in this 15 bit message. These 11 bits contain information while the left 4 bits' function is error correcting.

Klein four-group

- V or K_4: the smallest non-cyclic group
- V is an Abelian group
- V is isomorphic to the direct product of Z_2: $Z_2 \times Z_2$
- V is a normal subgroup of the alternating group A_4 (and also the symmetric group S_4) on four letters. In fact, it is the kernel of a surjective group homomorphism from S_4 to S_3: $V = \{(e), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$
- In music composition the four-group is the basic group of permutations in the twelve-tone technique.

	e	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*c*	*b*
b	*b*	*c*	*e*	*a*
c	*c*	*b*	*a*	*e*

Quaternion

- Quaternions are a number system that extends the complex numbers. They were first described by Irish mathematician William Rowan Hamilton in 1843 and applied to mechanics in three-dimensional space.
- Quaternions are generally represented in the form:

  $$a + bi + cj + dk$$

- where a, b, c, and d are real numbers, and i, j, and k are the fundamental quaternion units.

×	1	*i*	*j*	*k*
1	1	*i*	*j*	*k*
i	*i*	–1	*k*	–*j*
j	*j*	–*k*	–1	*i*
k	*k*	*j*	–*i*	–1

Quaternion group

- The center and the commutator subgroup of Q_8 is the subgroup {e,e}.
- The factor group Q_8/{e,e} is isomorphic to the Klein four-group V.
- The inner automorphism group of Q_8 is isomorphic to Q_8 modulo its center, and is therefore also isomorphic to the Klein four-group.
- The full automorphism group of Q_8 is isomorphic to the symmetric group of degree 4, S_4, the symmetric group on four letters.
- The outer automorphism group of Q_8 is then S_4/V which is isomorphic to S_3.

×	e	$\bar{e}$	i	$\bar{i}$	j	$\bar{j}$	k	$\bar{k}$
e	e	$\bar{e}$	i	$\bar{i}$	j	$\bar{j}$	k	$\bar{k}$
$\bar{e}$	$\bar{e}$	e	$\bar{i}$	i	$\bar{j}$	j	$\bar{k}$	k
i	i	$\bar{i}$	$\bar{e}$	e	k	$\bar{k}$	$\bar{j}$	j
$\bar{i}$	$\bar{i}$	i	e	$\bar{e}$	$\bar{k}$	k	j	$\bar{j}$
j	j	$\bar{j}$	$\bar{k}$	k	$\bar{e}$	e	i	$\bar{i}$
$\bar{j}$	$\bar{j}$	j	k	$\bar{k}$	e	$\bar{e}$	$\bar{i}$	i
k	k	$\bar{k}$	j	$\bar{j}$	$\bar{i}$	i	$\bar{e}$	e
$\bar{k}$	$\bar{k}$	k	$\bar{j}$	j	i	$\bar{i}$	e	$\bar{e}$

Rubik's cube

- The breakthrough, known as "descent through nested sub-groups" was found by Morwen Thistlethwaite; details of Thistlethwaite's algorithm were published in Scientific American in 1981 by Douglas Hofstadter.

The approaches to the cube that led to algorithms with very few moves are based on group theory and on extensive computer searches. Thistlethwaite's idea was to divide the problem into subproblems. Where algorithms up to that point divided the problem by looking at the parts of the cube that should remain fixed, he divided it by restricting the type of moves that could be executed. In particular he divided the cube group into the following chain of subgroups:

$$G_0 = \langle L, R, F, B, U, D \rangle$$
$$G_1 = \langle L, R, F, B, U^2, D^2 \rangle$$
$$G_2 = \langle L, R, F^2, B^2, U^2, D^2 \rangle$$
$$G_3 = \langle L^2, R^2, F^2, B^2, U^2, D^2 \rangle$$
$$G_4 = \{e\}$$

A random cube is in the general cube group G_0. Next he found this element in the right coset space $G_1 \backslash G_0$, et al.,

Symmetric group

- S_n the group of all the permutation of n letters, so the order of S_n is n!;
- The elements of the symmetric group on a set X are the permutations of X;
- The group operation in a symmetric group is function composition (not commutative for n>2);
- Transposition: permutation which exchanges two elements and keeps all others fixed
  - Every permutation can be written as a product of transpositions; for instance, the permutation (1 5 2)(3 4) can be written as g = (1 2)(2 5)(3 4)
  - Odd/even permutation: a permutation can be written as a product of an odd/even number of transpositions (not unique)
  - Sign of a permutation: +1 for even; -1 for odd (useful in calculating matrix determinant)
  - Sgn: $S_n \rightarrow$ {+1,-1} is a group homomorphism ({+1, –1} is a group under multiplication, where +1 is e, the neutral element)

- Alternating group A_n: the kernel of the homomorphism Sgn: $S_n \rightarrow \{+1,-1\}$, i.e. the set of all even permutations, is called the alternating group A_n. It is a normal subgroup of S_n, and for $n \geq 2$ it has $n!/2$ elements;
- Every permutation can be written as a product of adjacent transpositions, that is, transpositions of the form (a, a+1).
  - E.g. The sorting algorithm Bubble sort is an application of this fact. The representation of a permutation as a product of adjacent transpositions is also not unique.
- The normal subgroups of the finite symmetric groups are well understood.
  - If $n \leq 2$, Sn has at most 2 elements, and so has no nontrivial proper subgroups.
  - The alternating group of degree n is always a normal subgroup, a proper one for $n \geq 2$ and nontrivial for $n \geq 3$;
  - For $n \geq 3$, A_n is in fact the only non-identity proper normal subgroup of Sn, except when n = 4 where there is one additional such normal subgroup, which is isomorphic to the Klein four group.
- $S_4 \rightarrow S_3$ corresponding to the exceptional normal subgroup $V < A_4 < S_4$;

- Cayley's theorem states that every group G is isomorphic to a subgroup of the symmetric group on G.
  - Z_2 = {0,1} with addition modulo 2; group element 0 corresponds to the identity permutation e, group element 1 to permutation (12). E.g. 0 +1 = 1 and 1+1 = 0, so 1 -> 0 and 0 -> 1, as they would under a permutation.
  - Z_3 = {0,1,2} with addition modulo 3; group element 0 corresponds to the identity permutation e, group element 1 to permutation (123), and group element 2 to permutation (132). E.g. 1 + 1 = 2 corresponds to (123)(123)=(132).
  - Z_4 = {0,1,2,3} with addition modulo 4; the elements correspond to e, (1234), (13)(24), (1432). The elements of Klein four-group {e, a, b, c} correspond to e, (12)(34), (13)(24), and (14)(23).

Symmetry group

- The symmetry group of an object (image, signal, etc.) is the group of all transformations under which the object is invariant with composition as the group operation.
- 2D case: Wallpaper groups

https://en.wikipedia.org/wiki/Wallpaper_group

- Space groups in 3D (Fedorov groups or crystallographic groups):

https://en.wikipedia.org/wiki/Space_group

Erlangen program

- Group action: https://en.wikipedia.org/wiki/Group_action
  - A mapping (function):

    $H \times G \rightarrow G$

    $(h, g) \rightarrow g \circ m$
  - is called a group action, if it satisfies identity and compatibility:
  - $e \circ g = g$; $h_1 \circ (h_2 \circ g) = (h_1 h_2) \circ g$
- Representation of group: actions of groups on vector spaces.
- Orbit and invariant
  - E.g. Similar transformation is one kind of group action: $GL_n(R) \times M_n(R) \rightarrow M_n(R)$; it doesn't change the matrix's trace and determinant:
  - If $A = XDX^{-1}$, where D is a diagonal matrix containing all the eigenvalues λ, then trace(A) = sum(λ);
  - Besides, det(A) = det(D) = product(λ)
  - https://en.wikipedia.org/wiki/Trace_(linear_algebra)
- Klein geometry: https://en.wikipedia.org/wiki/Klein_geometry

Galois theory

- At the level of groups of symmetries of zeroes, in order for an equation to be solvable by radicals, it has to have such a chain of subgroups (or called extended Fields):

$$G_1 \supseteq G_2 \supseteq \ldots \supseteq G_k = E = \{e\}$$

- with properties that
- 1) G_i is a normal subgroup of G_{i+1}, for every i=1,2,…,k-1;
- 2) The corresponding quotient group G_{i+1}/G_i is isomorphism to the cyclic group (i.e. $x^p=c$)

Example: $x^4+px^2+q=0$

- The roots of this equation:

$$x_1 = \sqrt{\frac{-p+\sqrt{p^2-4q}}{2}}, \quad x_2 = -\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}}$$

$$x_3 = \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}, \quad x_4 = -\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}$$

- Denote R=Q(p, q) as the field (no forms of square root) of all radicals of p and q;
- Then, there are only two relations:

$$x_1+x_2=0; \qquad x_3+x_4=0$$

- The corresponding (normal) subgroup of the permutation group of roots is:

D_4 = {e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)} $\subseteq$ S_4

- If we introduce variable w with the form of square root: w is a root in cyclic equation $w^2=p^2-4q$, then the field is extended as R'=R(w), which denotes the radicals using p, q and $w=\mathrm{sqrt}(p^2-4q)$.
- Then, one more relation occurs:

$$x_1^2 - x_3^2 = w$$

- Corresponding normal subgroup:

$$K = \{e, (12), (34), (12)(34)\} \subseteq D_4$$

- If we introduce one more variable $u^2=(-p-w)/2$, then we have a new extended field R''=R'(u), with the new relation:

$$x_3 - x_4 = 2u$$

- The corresponding normal subgroup is:

$$Z_2 = \{e, (12)\} \subseteq K$$

- Then, one more variable $v^2 = (-p+w)/2$, and extended field R''' = R''(v), with the relation:

$$x_1 - x_2 = 2v$$

- It is invariant only in the group $E = \{e\} \subseteq Z_2$
- So the fields and subgroups chains are:

$$\begin{array}{cccccccc} & R''(v) & & R'(u) & & R(w) & & \\ R''' & \supseteq & R'' & \supseteq & R' & \supseteq & R \\ E & \subseteq & Z_2 & \subseteq & K & \subseteq & D_4 \end{array}$$

Solve this linear system:

$$\begin{cases} x_1 + x_2 = 0 \\ x_3 + x_4 = 0 \\ x_3 - x_4 = u(w) \\ x_1 - x_2 = v(w) \end{cases}$$

We can get the roots expressed as rational functions of coefficients of the original equation.

- If n=5: $S_5 \supseteq A_5 \supseteq E$, unsolvable
  - Where E is the only normal subgroup of A_5, which is not cyclic.
- If n=4: $S_4 \supseteq A_4 \supseteq K \supseteq Z_2 \supseteq E$, solvable
- If n=3: $S_3 \supseteq A_3 \supseteq Z_3 \supseteq E$, solvable
- If n=2: $S_2 \supseteq E$, solvable

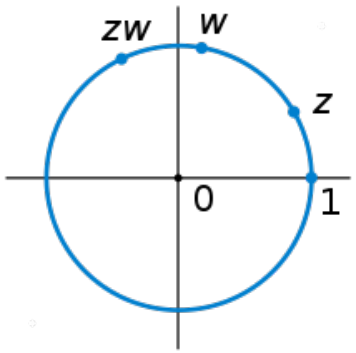
Lie group and Lie algebra

- Sophus Lie (1842-1899, Norwegian mathematician)
- Galois group dealing with polynomial equations → Lie group dealing with differential equations
  - Algebraic equations: discrete symmetry, permutation groups
  - Differential equations: continuous symmetry, Lie groups
- Examples
  - $GL_2(R)$
  - $SL_2(R)$ or SO(2)
  - SO(3)
  - Matrix groups in GL(n):

    SL(n): det(M)=1

    Orthogonal matrix: $M^T M = I$

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} = \frac{1}{1+t^2}\begin{pmatrix} 1-t^2 & -2t \\ 2t & 1-t^2 \end{pmatrix}$$



References

- Steven A. Leduc: Cracking the GRE Mathematics Subject Test, 2nd edition. Chapter 6.
- A. D. Aleksandrov, A. N. Kolmogorov, M. A. Lavrent'ev: Mathematics, its content, methods and meaning.
- 杨子胥：近世代数（第二版）
- 石明生：近世代数初步
- Math history: https://www.youtube.com/watch?v=dW8Cy6WrO94&list=PL55C7C83781CF4316
- Wikipedia