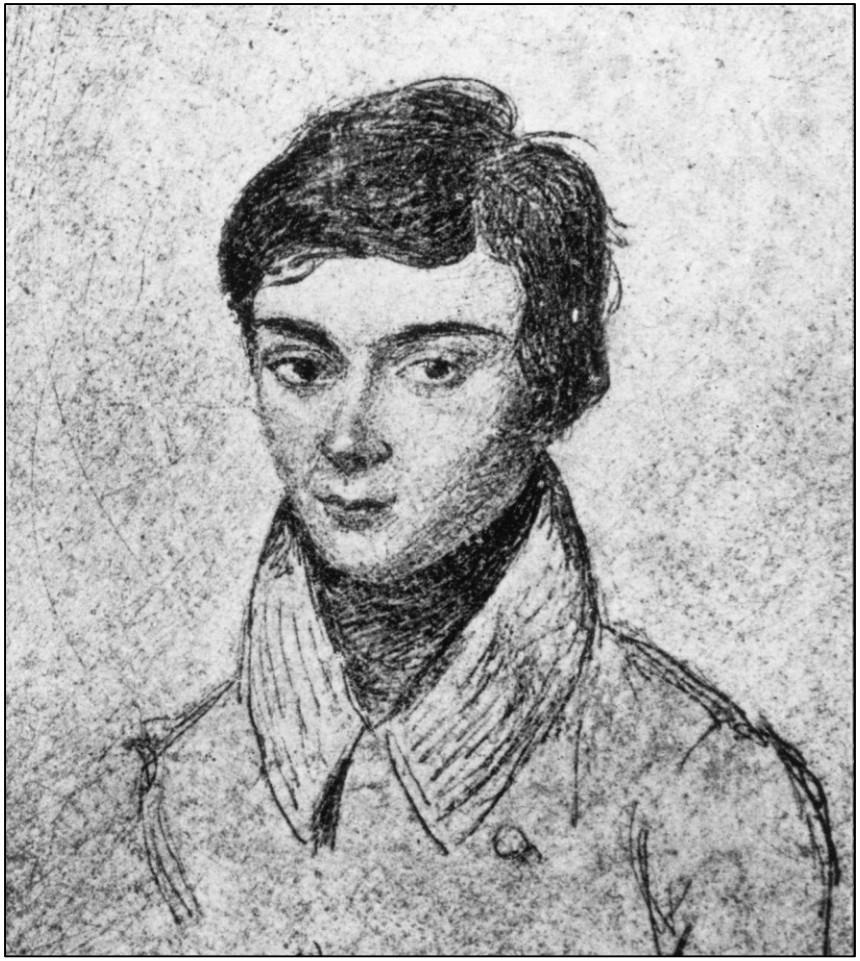
Group Theory

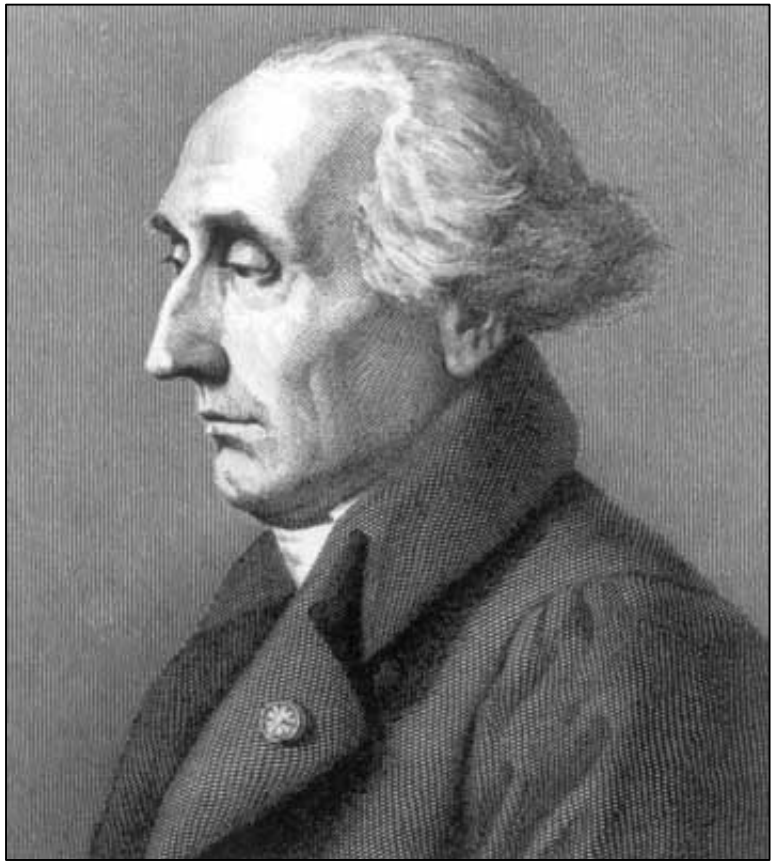
- Some of you facing difficulties in realizing a bit of new stuff, however, please TRY!!

Évariste Galois (1811-1832)



- Would-be revolutionary, expelled from school
- Studied math on his own
- Died in a pointless duel
- Wrote a letter that planted the seeds of group theory the night before his death

Joseph-Louis Lagrange (1736-1813)



- Leading mathematician in Europe at the time
- Contributed to many areas of mathematics and physics
- Lived in Italy, Germany, and France
- Involved in creation of the metric system

Divisibility and Divisors

- We say that ***m* divides *n*** (or ***n* is divisible by *m)*** if:
  - $m > 0$

  and:
  - the ratio $\frac{n}{m}$ is an integer.

- This property underlies all number theory, so we have a notation for it:

$$m \mid n$$

  and we say that *m* is a ***divisor*** of *n*

Prime Numbers

- Primes are important because they form the fundamental building blocks of all the positive integers:
  - Any positive integer n can be written as a ***product of primes***:

$$n = p_1 \cdot p_2 \cdot \ldots p_m = \prod_{k=1}^{m} p_k \qquad (p_1 \le p_2 \le \cdots \le p_m)$$

    and ***this expansion is unique*** – there is only one way to write n as a product of primes in non-decreasing order.

- This is known as the ***Fundamental Theorem of Arithmetic***

Greatest Common Divisor (GCD)

- The ***greatest common divisor*** of two integers m and n is the largest integer that divides them both:

  gcd(m, n) = max{k | $k|m$ and $k|n$}

  – Euclid's algorithm to calculate gcd(m,n), for given values $0 \le m \le n$ uses the recurrence:

$$\gcd(0, n) = n;$$

$$\gcd(m, n) = \gcd(n \bmod m, m), \qquad \text{for } m > 0$$

- So, for example, gcd(12, 18) = gcd(6,12) = gcd(0,6) = 6
  – Because any common divisor of m and n must also be a common divisor of both m and the number:

$$n \bmod m = n - \lfloor n / m \rfloor m$$

where $\lfloor a \rfloor$ is the *floor* function, the smallest integer less than or equal to a

Binary operation

A *binary operation* on a set is a rule for combining two elements of the set. More precisely, if S is a non-empty set, a binary operation on S is a mapping $f : S \times S \rightarrow S$. Thus f associates with each ordered pair (x,y) of element of S an element f(x,y) of S. It is better notation to write x * y for f(x,y), referring to as the binary operation.

The operations in a group follow the requirements of a mathematical group.

- Closure
- Identity
- Associativity
- Reciprocality

Groups

- A ***group***, G, is a *set of elements with an associated binary operation*, $\bullet$. It is sometimes denoted $\{G, \bullet\}$
  - For each ordered pair (a, b) of elements in G, there is an associated element ($a \bullet b$), such that the following axioms hold:

1) ***Closure*** : If a and $b \in G$, then $a \bullet b \in G$

2) ***Associative*** : $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a,\ b,\ c \in G$

3) ***Identity element*** : There is an element $e \in G$ such that
$a \bullet e = e \bullet a = a$ for all $a \in G$

4) ***Inverse element*** : For each $a \in G$ there is an element $a' \in G$ such that
$a \bullet a' = a' \bullet a = e$

Groups

- A ***finite group*** is a group with a finite number of elements, otherwise, a group is an ***infinite group***.
- A group is said to be an ***abelian group*** if it satisfies the following condition:

5) ***Commutativ e*** : $a \bullet b = b \bullet a$ for all $a,\ b \in G$

– Examples of abelian groups:

- The set of integers (negative, zero, and positive), ***Z***, under addition.
  The identity element of ***Z*** under addition is 0;
  the inverse of a is -a, for all a in ***Z***.
- The set of non-zero real numbers, ***R****, under multiplication.
  The identity element of ***R**** under multiplication is 1;
  the inverse of a is $1/a$ for all a in ***R****.

Example

Let me describe the addition and multiplication on $\mathbb{Z}_4$ by tables:

Addition Table				
$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Product Table				
$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Let me do the same for $\mathbb{Z}_5$:

Addition Table					
$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Product Table					
$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Exponentiation and Cyclic Groups

- ***Exponentiation*** within a group is repeated application of the group operator, such that:

  $a^0 = e$, the identity element

  $a^n = a \bullet a \bullet \cdots \bullet a$ (i.e. $\bullet$ applied n-1 times)

  $a^{-n} = (a')^n$, where a' is the inverse of a

- A group G is ***cyclic*** if every element of G is a power g^k (k is an integer) of a fixed element $g \in G$. The element g is said to ***generate the group***, or to be ***a generator of the group***.
- A cyclic group is always abelian, and may be finite or infinite
  - Example of a cyclic group:
    - The group of positive integers, $\{\boldsymbol{N}, +\}$, ($\boldsymbol{N} = \{1, 2, 3, ...\}$) under addition is an infinite cyclic group generated by the element 1. (i.e. 1 + 1 = 2, 1 + 1 + 1 = 3, etc.)

Proposition. If *a, b, and c are elements of a group G, then*

(i) $(a^{-1})^{-1} = a$.

(ii) $(ab)^{-1} = b^{-1}a^{-1}$.

(iii) *ab = ac or ba = ca implies that b = c. (cancellation law)*

Subgroups

It often happens that some subset of a group will also form a group under the same operation.Such a group is called a *subgroup*. If (G, ▪) is a group and H is a nonempty subset of G, then (H, ▪) is called a *subgrou*p of (G, ▪) if the following conditions hold:

(i) $a \blacksquare b \in H$ for all $a, b \in H$. (*closure*)

(ii) $a^{-1} \in H$ for all $a \in H$. (*existence of inverses*)

Multiplicative group of nonzero remainders mod 7 – what makes it a group?

×	1	2	3	4	5	6	
1	**1**	2	3	4	5	6	1
2	2	4	6	**1**	3	5	4
3	3	6	2	5	**1**	4	5
4	4	**1**	5	2	6	3	2
5	5	3	**1**	6	4	2	3
6	6	5	4	3	2	**1**	6

{1, 2, 3, 4, 5, 6}

- Has binary group operation (multiplication)
- Has an identity element (product of *x* and 1 is *x*)
- Closed under multiplication, e.g. $4 \circ 3 = (4 \times 3) \bmod 7 = 5$
- Closed under inverse, e.g. $5^{-1} = 3 \bmod 7$

Lagrange's Theorem

The order of any element in a finite group divides the order of the group.

Proof:

- The powers of an element of *G* form a subgroup of *G*.
- Since the order of an element is the order of the subgroup, and since the order of the subgroup must divide the order of the group, then the order of the element must divide the order of the group.

Cyclic subgroup

- If G is a group and a $\in$ G, write

  $<a> = \{a^n : n \in Z\} = \{\text{all powers of a}\}$.

  It is easy to see that $<a>$ is a subgroup of G .

  $<a>$ is called the *cyclic subgroup* of G generated by a. A group G is called *cyclic* if there is some a $\in$ G with $G = <a>$; in this case a is called a *generator* of G.

- **Proposition:** *If* $G = <a>$ *is a cyclic group of order n, then* a^k *is a generator of G if and only if gcd(k; n)= 1.*
- **Corollary:** *The number of generators of a cyclic group of order n is* $\phi(n)$.

Cosets

- Let $(G, \cdot)$ be a group with subgroup H. For a, b ∈ G, we say that a is ***congruent to b modulo H***, and write **a ≡ b mod H** if and only if $ab^{-1} \in H$.

- **Find the right cosets of A_3 in S_3.**

Solution. One coset is the subgroup itself $A_3 = \{(1), (123), (132)\}$. Take any element not in the subgroup, say (12). Then another coset is $A_3(12) = \{(12), (123)\ (12), (132)\ (12)\} = \{(12), (13), (23)\}$.Since the right cosets form a partition of S_3 and the two cosets above contain all the elements of S_3, it follows that these are the only two cosets.

In fact, $A_3 = A_3(123) = A_3(132)$ *and* $A_3(12) = A_3(13) = A_3(23)$.

Normal subgroups

Definition: A subgroup H of a group G is called a *normal subgroup* of G if $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$.

Proposition 2.3.1. *Hg = gH, for all $g \in G$, if and only if H is a normal subgroup of G.*

Proof. Suppose that Hg = gH. Then, for any element $h \in H$, $hg \in Hg = gH$. Hence $hg = gh_1$ for some $h_1 \in H$ and $g^{-1}hg = g^{-1}gh_1 = h_1 \in H$. Therefore, H is a normal subgroup.

Conversely, if H is normal, let $hg \in Hg$ and $g^{-1}hg = h_1 \in H$. Then $hg = gh_1 \in gH$ and $Hg \subseteq gH$. Also, $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = h_2 \in H$, since H is normal, so $gh = h_2g \in Hg$. Hence, $gH \subseteq Hg$, and so Hg = gH.

Rings

- A ***ring***, R, denoted by $\{R, +, \times\}$, is a set of elements with two binary operations, called ***addition*** $(+)$ ***and multiplication*** $(\times)$, such that, for a, b, c in R:

addition and ***multiplication*** are abstract operations here

1)-5) ***R is an abelian group with respect to addition***; for this case of an additive group, we denote the identity element as 0, and the inverse of a as $-a$.

6) ***Closure under multiplication:***

If a and b belong to R, then $a \times b$ is also in R

7) ***Associativity of multiplication:***

$a \times (b \times c) = (a \times b) \times c$ for all a, b, c, in R

8) ***Distributive Laws:***

$a \times (b + c) = a \times b + a \times c$ for all a, b, c, in R

$(a + b) \times c = a \times c + b \times c$ for all a, b, c, in R

Note that we often write $a \times b$ as simply ab

Commutative Rings

- A ring is ***commutative*** if it satisfies the following additional condition:

9) ***Commutativity of multiplication:***

$a \times b = b \times a$ for all a, b, c, in R

Example of a commutative ring:

The set of even integers, {..., -4, -2, 0, 2, 4, ...}) under the normally defined integer operations of addition and multiplication.

Integral Domains

- An ***integral domain*** is a commutative ring that obeys the following:

10) ***Multiplicative identity:***

There is an element 1 in R such that $a \times 1 = 1 \times a = a$ for all a in R

11) ***No zero divisors:***

If a, b in R and $a \times b = 0$, then either $a = 0$ or $b = 0$

Example of an integral domain:

The set of all integers ($\boldsymbol{Z}$ = {..., -3, -2, -1, 0, 1, 2, 3, ...}) under the normally defined integer operations of addition and multiplication, {$\boldsymbol{Z}$, +, ×}

×

Fields

- A ***field***, F, denoted by $\{F, +, \times\}$, is a set of elements with two binary operations, called *addition* and *multiplication*, such that, for all a, b, c in F, the following apply:

Again, ***addition*** and ***multiplication*** are abstract operations

1)-11) ***F is an integral domain***

11) ***Multiplicative inverse:***

For each a in F, except 0, there is an element a^{-1} in F such that:

$$a \times a^{-1} = a^{-1} \times a = 1$$

Fields

- A field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set.
- Division is defined:

$$a/b = a(b^{-1})$$

Examples:

- The set of rational numbers, ***Q***; the set of real numbers, ***R***, the set of complex numbers, ***C***.
- The set of all integers, ***Z***, is *not* a field, because only the elements 1 and -1 have multiplicative inverses in the integers.

Groups, Rings, and Fields