Introduction to Abstract Algebra Notes

Francesco Chotuck

]

Contents

1 The Integers

1.1 The Division Algorithm

Definition 1.1. We say that m is **divisible** by n or that n **divides** m if $m = nk$ for some $k \in \mathbb{Z}$. It is written as $n|m$ and read as "n divides m."

Proposition 1. Suppose that $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$.

1. If $a|b$ and $b|c$, then $a|c$.
2. If $a|n$, then $a \leq n$.
3. If $n|a$ and $n|b$, then $n|(ac + bd)$.

Theorem 1.1. (The Division Algorithm) Suppose that $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then there exists $q, r \in \mathbb{Z}$ such that both of the following hold:

1. $m = qn + r$, and
2. $0 \leq r < n$.

Note that r is called the **remainder**. Moreover, q and r are the unique pair of integers such that these hold.

Remark. *In general m and $m + kn$, for $k \in \mathbb{Z}$, have the same remainder on division by n.*

1.2 The Euclidean Algorithm

Definition 1.2. Suppose a and b are integers, not both zero. Then the **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the greatest integer which divides both a and b. Thus $g = \gcd(a, b)$ if the following hold:

1. $g|a$ and $g|b$,
2. If $d|a$ and $d|b$, then $d \leq g$.

Theorem 1.2. Suppose that $a, b \in \mathbb{Z}$ and that a and b are not both zero, and let $g = \gcd(a, b)$. Then

1. g is the least positive integer of the form $ax + by$ with $x, y \in \mathbb{Z}$;
2. if $d|a$ and $d|b$, then $d|g$.

Proposition 2. If $a, b, c, k \in \mathbb{Z}$ with $b \neq 0$ and $a = kb + c$, then $\gcd(a, b) = \gcd(b, c)$.

Example. Work out the $\gcd(114, 42)$.
Solution: By using the Euclidean Algorithm.

$$\begin{aligned}114 &= 2 \cdot 42 + 30\\ 42 &= 1 \cdot 30 + 12\\ 30 &= 2 \cdot 12 + 6\\ 12 &= 2 \cdot 6 + 0.\end{aligned}$$

The last non-zero remainder is 6 therefore, $\gcd(114, 42) = 6$.

Example. We can "unwind" the Euclidean Algorithm to obtain an the equation $ax + by = g = \gcd(a, b)$ for $a, b, x, y, g \in \mathbb{Z}$. Using the equations from Example 1.2 gives:

$$\begin{aligned}6 &= 30 - 2 \cdot 12\\ 12 &= 42 - 30\\ 30 &= 114 - 2 \cdot 42.\end{aligned}$$

Substituting each equation into the previous one gives:

$$\begin{aligned}6 &= 30 - 2 \cdot 12\\ &= 30 - 2(42 - 30)\\ &= 3 \cdot 30 - 2 \cdot 42\\ &= 3(114 - 2 \cdot 42) - 2 \cdot 42\\ &= 3 \cdot 114 - 8 \cdot 42.\end{aligned}$$

Therefore we have $6 = \gcd(114, 42) = 114x + 42y$ by taking $x = 3$ and $y = -8$.

1.3 Relatively prime integers

Definition 1.3. Suppose that $a, b \in \mathbb{Z}$ and that a and b are not both zero. We say that a and b are **relatively prime** if $\gcd(a, b) = 1$.

Corollary 1.2.1. *Suppose that $a, b \in \mathbb{Z}$, not both 0. Then a and b are relatively prime if and only if $ax + by = 1$ for some $x, y \in \mathbb{Z}$.*

Corollary 1.2.2. *Suppose that $a, b \in \mathbb{Z}$, not both 0. Let $g = \gcd(a, b)$. Then a/g and b/g are relatively prime.*

Corollary 1.2.3. *Suppose that $a, b, c \in \mathbb{Z}$ with a and b relatively prime. If $a|bc$, then $a|c$.*

Remark. *We can think of Corollary 1.2.3 in the following formulation: if a and b are relatively prime and $a|bc$, then a cannot divide into b hence, it must divide c.*

Corollary 1.2.4. *Suppose that $a, b, c \in \mathbb{Z}$ with a and b relatively prime. If $a|c$ and $b|c$, then $ab|c$.*

1.4 Linear Diophantine equations

Definition 1.4. A **linear Diophantine equation** (in two variables) is an equation of the form

$$ax + by = c,$$

where $a, b, c \in \mathbb{Z}$ and we regard x and y as variables taking only integer values.

Theorem 1.3. Suppose that $a, b, c \in \mathbb{Z}$ and that a and b are not both zero. Then the equation $ax + by = c$ has solutions $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b)|c$.

Theorem 1.4. Suppose that $a, b, c \in \mathbb{Z}$ and that $g = \gcd(a, b)$. If $x = x_0, y = y_0$ is an integer solution to $ax + by = c$, then all the integer solutions of $ax + by = c$ are given by

$$\begin{aligned} x &= x_0 + k\left(\frac{b}{g}\right), \\ y &= y_0 - k\left(\frac{a}{g}\right) \quad \text{for } k \in \mathbb{Z}. \end{aligned}$$

Example. You're at a shop in the airport about to leave New York. You want to spend the last \$15 of your US money on chocolate by buying a combination of Mercury bars, which cost 39 cents apiece, and Andromeda bars, which cost 47 cents apiece. How many of each do you need to buy so you won't have any change?
Solution: Let x be the number of Mercury bars and y the number of Andromeda bars. We have to solve the equation

$$39x + 47y = 1500$$

where x and y are non-negative integers. By the Euclidean Algorithm we have that $g = \gcd(39, 47) = 1$ therefore,

$$39x_0 + 47y_0 = 1500$$

with $x_0 = -9000$ and $y_0 = 7500$. Hence, all the solutions are

$$\begin{aligned} x &= -9000 + 47k, \\ y &= 7500 - 39k \end{aligned}$$

for $k \in \mathbb{Z}$. But we require x and y to be non-negative integers so, the solutions must satisfy

$$\begin{aligned} x &= -9000 + 47k \geq 0 \\ y &= 7500 - 39k \geq 0. \end{aligned}$$

This is equivalent to $k \geq 9000/47 \approx 191.5$, and $k \leq 7500/39 \approx 192.3$. Therefore the only possible value of k is 192, giving $x = 24$ and $y = 12$.

1.5 Prime factorisation

Definition 1.5. Suppose that n is an integer and $n > 1$. Then n is **prime** if its only positive divisors are 1 and n; otherwise n is **composite.**

Proposition 3. Suppose that $a, b \in \mathbb{Z}$ and p is a prime number. If $p|ab$ then $p|a$ or $p|b$.

Corollary 1.4.1. *Suppose that $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ and p is a prime number. If $p|a_1a_2 \ldots a_k$ then $p|a_i$ for some $i \in \{1, 2, \ldots, k\}$.*

Theorem 1.5. (The Fundamental theorem of Arithmetic). Suppose that n is an integer greater than 1. Then there is a positive integer k and prime numbers $p_1, p_2, \ldots, p_k$ such that $n = p_1p_2 \ldots p_k$. Moreover the factorization is unique, up to changing the order of the prime factors $p_1, p_2, \ldots, p_k$.

Corollary 1.5.1. *Suppose that m and n are integers, not both 0. Then m and n are relatively prime if and only if they have no common prime divisors.*

Corollary 1.5.2. *Suppose that $p_1, p_2, \ldots, p_k$ are distinct prime numbers and $r_1, r_2, \ldots, r_k$ and $s_1, s_2, \ldots, s_k$ are non-negative integers. Let $m = p_1^{r_1}p_2^{r_2} \ldots p_k^{r_k}$ and $n = p_1^{s_1}p_2^{s_2} \ldots p_k^{s_k}$.*

1. *Then $n|m$ if and only if $s_1 \leq r_1, s_2 \leq r_2, \ldots, s_{k-1} \leq r_{k-1}$ and $s_k \leq r_k$.*

2. *$\gcd(m, n) = p_1^{t_1}p_2^{t_2} \ldots p_k^{t_k}$ where $t_1 = \min(r_1, s_1), t_2 = \min(r_2, s_2), \ldots, t_{k-1} = \min(r_{k-1}, s_{k-1})$ and $t_k = \min(r_k, s_k)$.*

3. *$\operatorname{lcm}(m, n) = p_1^{t_1}p_2^{t_2} \ldots p_k^{t_k}$ where $t_1 = \max(r_1, s_1), t_2 = \max(r_2, s_2), \ldots, t_{k-1} = \max(r_{k-1}, s_{k-1})$ and $t_k = \max(r_k, s_k)$.*

2 Binary operations

2.1 Arithmetic modulo n

Definition 2.1. Suppose that a and b are integers. We say that a is **congruent** to b **modulo** n if $a - b$ is divisible by n. The notation for this is $a \equiv b \pmod{n}$.

Proposition 4. Suppose that a, b and n are integers and $n > 0$. Then the following are equivalent:

(a) $a \equiv b \pmod{n}$;

(b) $a = b + kn$ for some $k \in \mathbb{Z}$;

(c) a and b have the same remainder on division by n.

Corollary 2.0.1. *If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

Proposition 5. Suppose that a, b, c, d and n are integers and $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

1. $a \pm c \equiv b \pm d \pmod{n}$, and
2. $ac \equiv bd \pmod{n}$.

Proposition 6. Suppose that $a, b, c, d \in \mathbb{Z}$ and $m, n \in \mathbb{N}$. If $a \equiv b \pmod{n}$,then $a^m \equiv b^m \pmod{n}$.

Definition 2.2. If $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, then we call the set

$$\{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$$

the **congruence** (or **residue**) **class** of a **modulo** n, and denote it by $[a]_n$.

Remark. *Definition 2.2 is equivalent as saying*

$$[a]_n = \{a + kn : k \in \mathbb{Z}\}.$$

Example.

$$[5]_{12} = \{b \in \mathbb{Z} : b \equiv 5 \pmod{n}\} = \{\ldots, -19, -7, 5, 17, \ldots\}.$$

Remark. *Since $a \equiv a \pmod{n}$ to get $[a]_n$ it suffices to add integer constants to a.*

Proposition 7. Suppose $a, b \in \mathbb{Z}, n \in \mathbb{N}$. Then

$$a \equiv b \pmod{n} \iff [a]_n = [b]_n.$$

Proposition 8. Suppose that $n \in \mathbb{N}$ and $a, b, a', b' \in \mathbb{Z}$. If $[a]_n = [a']_n$ and $[b]_n = [b']_n$, then $[a + b]_n = [a' + b']_n$ and $[ab]_n = [a'b']_n$.

Definition 2.3. Let $\mathbb{Z}_n$ denote the set of congruence classes modulo n, so:

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

is a set with n elements; each element of $\mathbb{Z}_n$ is itself a set of infinitely many integers.

Proposition 9. The addition and multiplication operations on $\mathbb{Z}_n$ are commutative and associative.

3 Groups

3.1 Definition of a group

Definition 3.1. A **group** is a set G with a binary operation $*$ satisfying the following properties:

1. $*$ is associative;
2. there is an element $e \in G$ such that $e * g = g * e = g$ for all $g \in G$;
3. if $g \in G$, then there is an element $h \in G$ such that $g * h = h * g = e$.

Remark. *By the definition of a binary operation the operation $*$ already satisfies the closure axiom.*

3.2 Example of groups

We write $(G, *)$ to express a group G with operation $*$.

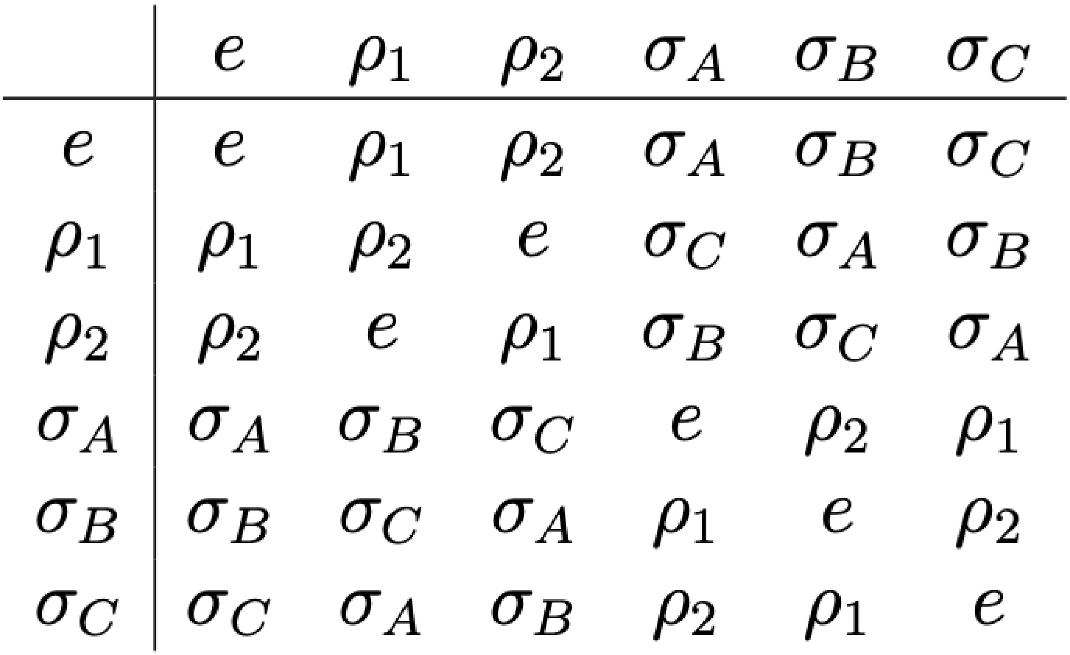
Example.

- $(\mathbb{Z}, +)$;
- $(\mathbb{R}^\times, \cdot)$ where $\mathbb{R}^\times = \mathbb{R} \backslash \{0\}$;
- $(M_2(\mathbb{R}), +)$;
- $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ where $\mathrm{GL}_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det(A) \neq 0\}$. This is called the "General linear" group;
- D_3 the set of symmetries of an equilateral triangle.

3.2.1 The D_3 group

Let D_3 denote the set of symmetries of an equilateral triangle. There are 6 of these:

- The identity, e;
- Two 120° rotations; call these ρ_1 (clockwise) and ρ_2 (anticlockwise);
- Three reflections (one axis through each vertex), call these σ_A, σ_B and σ_C (ordering the vertices clockwise.)



	e	ρ_1	ρ_2	σ_A	σ_B	σ_C
e	e	ρ_1	ρ_2	σ_A	σ_B	σ_C
ρ_1	ρ_1	ρ_2	e	σ_C	σ_A	σ_B
ρ_2	ρ_2	e	ρ_1	σ_B	σ_C	σ_A
σ_A	σ_A	σ_B	σ_C	e	ρ_2	ρ_1
σ_B	σ_B	σ_C	σ_A	ρ_1	e	ρ_2
σ_C	σ_C	σ_A	σ_B	ρ_2	ρ_1	e

Figure 1: Cayley table of D_3

Proposition 10. The D_3 group is not cyclic.

Proposition 11. The D_3 group is not abelian.

Proposition 12. The group D_3 is isomorphic to S_3.

Remark. *The order of the Dihedral group n is given by $2n$.*

3.2.2 The $\mathbb{Z}_n$ groups

The $(\mathbb{Z}_n, +)$ is a group.

Proposition 13. Suppose $a, n \in \mathbb{Z}$ with $n \geq 1$. Then $[a]_n$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.

Proposition 14. Suppose that $a, b, n \in \mathbb{Z}$ with $n > 0$. If $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

Definition 3.2. We define the set $\mathbb{Z}_n^\times = \{[a]_n : \gcd(a, n) = 1\}$.

Proposition 15. $(\mathbb{Z}_n^\times, \cdot)$ is a group.

3.3 Permutation groups

Definition 3.3. For any set A, we define the **identity function** on A as the function

$$\mathrm{id}_A : A \to A, \quad \text{where } \mathrm{id}_A(a) = a \text{ for all } a \in A.$$

Definition 3.4. Suppose that f is a function from A to B. We say that a function $g : B \to A$ is an **inverse function** of f if

$$g \circ f = \mathrm{id}_A \quad \text{and} \quad f \circ g = \mathrm{id}_B\,.$$

Definition 3.5. Suppose that f is a function from A to B. We say f is **injective** if it has the following property:

$$x, y \in A, \quad f(x) = f(y) \Rightarrow x = y.$$

Definition 3.6. Suppose that f is a function from A to B. We say f is **surjective** if it has the following property:

$$b \in B \Rightarrow b = f(a) \quad \text{for some } a \in A.$$

Definition 3.7. A function $f : A \to B$ is bijective if it is both injective and surjective.

Proposition 16. Suppose that $f : A \to B$ and $g : B \to C$ are functions.

1. If f and g are injective, then so is $g \circ f$.
2. If f and g are surjective, then so is $g \circ f$.
3. If f and g are bijective, then so is $g \circ f$.

Theorem 3.1. Suppose that $f : A \to B$ is a function. Then f has an inverse function if and only if f is bijective.

Definition 3.8. We define S_A to be the set of bijective functions from A to A.

Proposition 17. If A is a set, then S_A is a group under $\circ$.

Remark. *The group S_A under $\circ$ is called the* ***symmetric group****, or* ***permutation group****, on A, and its elements are called* ***permutations*** *of A.*

Proposition 18. There are $n!$ elements in S_n.

Proposition 19. The order of σ when it is made up of disjoin cycles, is the lcm of the cycle length of each disjoint cycle.

There are two standard ways of denoting elements of S_n. One of these is to write

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

for the function (or permutation) $\sigma \in S_n$ such that $\sigma(1) = a_1, \sigma(2) = a_2, \dots, \sigma(n) = a_n$.

The other standard notation is **cycle notation**. If $a_1, a_2, \dots, a_k$ are distinct elements of $\{1, 2, \dots, n\}$ (so $k \leq n$), we write

$$(a_1 a_2 \dots a_k).$$

An element of S_n of the form $(a_1 a_2 \dots a_k)$ is called a k-**cycle** (or just a **cycle**).

3.4 Cycle composition

TO DO!!

3.4.1 Cycle decomposition

Definition 3.9. Disjoint cycles have no cycle elements in common.

Example. For example $(1, 2, 3)$ and $(4, 5, 6, 7)$ are disjoint cycles. By contrast, $(1, 2, 3)$ and $(3, 4, 5, 6)$ are not disjoint because they have the 3 in common.

Example.

Ex Let $\sigma = (1,7,3)(1,5) \in S_7$. Write the decomposition of σ into disjoint cycles

$(\underline{\underline{1}},7,3)$ & $(\underline{\underline{1}},5)$ are **Not** **disjoint**.

Let's see what σ does to $\{1,\dots,7\}$.

$$\sigma = \underbrace{(1,7,3)}_{\alpha}\underbrace{(1,5)}_{\beta} = \alpha\beta$$

$\sigma(1) = \alpha\beta(1) = \alpha(\beta(1)) = \alpha(5) = 5$

$\sigma(2) = \alpha\beta(2) = \alpha(\beta(2)) = \alpha(2) = 2$

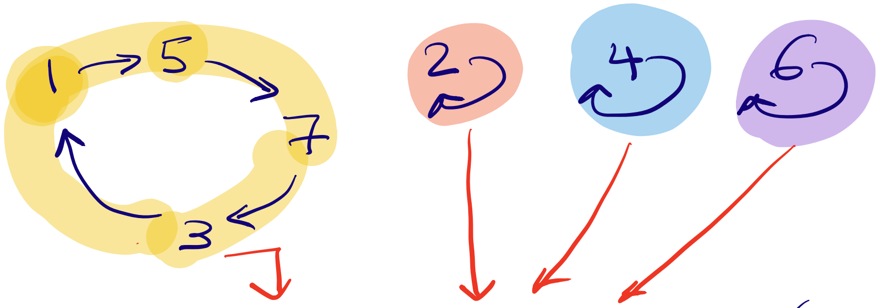
$\sigma(3) = \alpha\beta(3) = \alpha(\beta(3)) = \alpha(3) = 1$

$\sigma(4) = \qquad = 4$

$\sigma(5) = \qquad = 7$

$\sigma(6) = \qquad = 6$

$\sigma(7) = \qquad = 3$

$\Rightarrow$ 

$= \sigma = (1,5,7,3)\ e\ e\ e = (1,5,7,3)$

So in fact σ is a cycle of length 4.

Note $\circ$ is not commutative on S_n. $(n>2)$

ex

$$\begin{array}{ccc} (1,2)(1,3) & \neq & (1,3)(1,2) \\ \shortparallel & & \shortparallel \\ (1,3,2) & \neq & (1,2,3) \end{array}$$

this sends $1 \mapsto 3$ ⟵ $(1,3,2)$

$(1,2,3)$ ⟶ this sends $1 \to 2$

However if σ, τ are disjoint cycles then $\sigma\tau = \tau\sigma$.

$$(1,2)(5,3,7) = (5,3,7)(1,2)$$

3.5 Basic properties of groups

Proposition 20. Suppose $(G, *)$ is a group and $a \in G$. Then there is a unique $b \in G$ such that $a * b = b * a = e$.

Definition 3.10. Suppose that $(G, *)$ is a group and $a \in G$. Then the inverse of a is the unique element $b \in G$ such that $a * b = b * a = e$; we denote this element by a^{-1}.

Definition 3.11. We say a group $(G, *)$ is an **abelian** group if the operation $*$ is commutative; i.e., $a * b = b * a$ for all $a, b \in G$.

Proposition 21. (Cancellation Law). Suppose that G is a group and $a, b, c \in G$. If $ab = ac$ or $ba = ca$, then $b = c$.

Corollary 3.1.1. *If G is a group and $a, b \in G$, then there is a unique $x \in G$ such that $ax = b$ and a unique $y \in G$ such that $ya = b$.*

Proposition 22. Suppose G is a group and $g, h \in G$. Then

1. If $ab = e$, then $a = b^{-1}$ and $b = a^{-1.}$
2. $(ab)^{-1} = b^{-1}a^{-1}$.
3. $(a^{-1})^{-1} = a$.

3.6 Powers of group elements

Definition 3.12. If $(G, *)$ is a group and $g \in G$, then we define the n^{th} power of g for positive integers n by

$$g^n = \underbrace{g * g * \ldots * g}_{n \text{ times}}$$

and set $g^0 = e$ and $g^n = \left(g^{-n}\right)^{-1}$ for $n < 0$. Such that g^n is defined for all $n \in \mathbb{Z}$.

Proposition 23. Suppose G is a group, $g \in G$ and $m, n \in \mathbb{Z}$. Then $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$.

Example. ADD EXAPLES !!

3.7 Orders of group elements

Definition 3.13. Let g be an element of a group G. We say that g has **finite order** (in G) if $g^n = e$ for some $n \in \mathbb{N}$. In that case the least $n \in \mathbb{N}$ such that $g^n = e$ is called the **order** of g. If no such positive integer n exists, we say that g has **infinite order**.

Remark. *The identity element of a group has order 1.*

Theorem 3.2. Suppose that g is an element of a group G.

1. If g has infinite order, then $g^n = e \iff n = 0$.

2. If g has finite order d, then $g^n = e \iff d|n$.

Corollary 3.2.1. *Suppose that g is an element of a group G.*

1. *If g has infinite order, then the powers of g are distinct; i.e., $g^m = g^n \iff m = n$.*

2. *If g has finite order d, then $g^m = g^n \iff m \equiv n \pmod{d}$.*

Definition 3.14. Suppose that G is a group. If G has infinitely many elements, we say G has **infinite order**. Otherwise we say G has **finite order**, and we define the order of G to be the number of elements in G.

Corollary 3.2.2. *If a group G has finite order, then so does every element of G.*

Proposition 24. Suppose that $a_1, a_2, \ldots, a_k$ are distinct elements of the set $\{1, 2, \ldots, n\}$, and let $\sigma = (a_1\, a_2\, \ldots\, a_k)$. Then

1. $\sigma^{-1} = (a_k\, a_{k-1}\, \ldots\, a_1)$.

2. σ has order k.

3.8 Subgroups

Definition 3.15. Suppose that $(G, *)$ is a group. A subset $H \subseteq G$ is called a **subgroup** of G if H, with the operation $*$, is a group.

Proposition 25. Suppose that $(G, *)$ is a group and $H \subseteq G$. Then H is a subgroup of G if and only if the following conditions are all satisfied:

1. $h, h' \in H \Rightarrow h * h' \in H$;

2. $e \in H$;

3. $h \in H \Rightarrow h^{-1} \in H$.

3.9 Cyclic groups

Proposition 26. Suppose that G is a group and $g \in G$. Then

$$H = \{g^n : n \in \mathbb{Z}\}$$

is a subgroup fo G.

Definition 3.16. If g is an element of a group G, then $\{g^n : n \in \mathbb{Z}\}$ is denoted $\langle g \rangle$ and called the **subgroup of G generated by g**.

Proposition 27. Suppose that g is an element of a group G.

1. If g has infinite order, then so does $\langle g \rangle$.

2. If g has order $d \in \mathbb{N}$, then so does $\langle g \rangle$.

Definition 3.17. Suppose that G is a group. We say that G is a **cyclic group** if $G = \langle g \rangle$ for some $g \in G$. If $G = \langle g \rangle$, then we say that g is a **generator** (of G).

Proposition 28. Suppose that G is a finite group of order n.

1. If $g \in G$, then g has order at most n.

2. G is cyclic if and only if G has an element of order n.

3. If G is cyclic and $g \in G$, then g is a generator of G if and only if g has order n.

Proposition 29. If G is a cyclic group, then G is abelian.

Theorem 3.3. Suppose that G is a group, $g \in G$ has order d, and $a \in \mathbb{Z}$. Then g^a has order $d/\gcd(a,d)$.

Corollary 3.3.1. *Suppose that $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then the element $[a]_n$ in $\mathbb{Z}_n$ has order $n/\gcd(a,n)$.*

Corollary 3.3.2. *Suppose that $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $[a]_n$ generates $\mathbb{Z}_n$ if and only if a and n are relatively prime.*

Theorem 3.4. Every subgroup of a cyclic group is cyclic.

Corollary 3.4.1. *If H is a subgroup of $\mathbb{Z}$, then*

$$H = \langle m \rangle = \{km : k \in \mathbb{Z}\}$$

for some $m \in \mathbb{Z}$.

3.10 Cosets

Definition 3.18. Suppose that $(G, *)$ is a group, H is a subgroup of G, and g is an element of G. The subset $g * H \subseteq G$ defined by

$$g * H = \{g * h : h \in H\}$$

is called a **left coset** of H in G.

Proposition 30. Suppose that G is a group, H is a subgroup of G, and g and g' are elements of G. Then the following are equivalent:

1. $g'H = gH$;

2. $g' \in gH$;

3. $g^{-1}g' \in H$.

Corollary 3.4.2. *Suppose that G is a group, H is a subgroup of G and g is an element of G. Then g is in exactly one left coset of H in G, namely gH.*

3.11 Lagrange's Theorem

Lemma 3.5. *Suppose that H is subgroup of a group G, and that H has finite order d. Then every left coset of H in G has d elements.*

Theorem 3.6. (Lagrange's Theorem). Suppose that G is a group of finite order. If H is a subgroup of G, then the order of G is divisible by the order of H. i.e.

$$\text{number of elements in } G = \text{number of left cosets} \times \text{size of each coset.}$$

Definition 3.19. If H is a subgroup of a group G, then the number of left cosets of H in G is called the **index** of H in G, and denoted $[G : H]$ i.e. we call the

$$\frac{\text{order of } G}{\text{order of } H} = \text{number of distinct left cosets of } H \text{ in } G.$$

Corollary 3.6.1. *Suppose that G is a group of finite order n, and that $g \in G$. Then the order of g is a divisor of n.*

Corollary 3.6.2. *Suppose that G is a group of order p, where p is a prime number. Then G is cyclic.*

Corollary 3.6.3. *Suppose that G is a group of order n, and g is an element of G. Then $g^n = e$.*

Theorem 3.7. (Fermat's Little theorem). Suppose that p is a prime number and a is an integer.

1. $a^p \equiv a \pmod{p}$;

2. if a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Example. Find the remainder of 50^{50} on division by 13.
Solution:

$$50 \equiv -2 \pmod{13} \Rightarrow (50)^{50} \equiv (-2)^{50} \pmod{13}.$$

By Fermat's Little theorem:

$$\begin{aligned} 13 \nmid -2 \Rightarrow (-2)^{13-1} &\equiv 1 \pmod{13} \\ (-2)^{50} &\equiv (-2)^{12}(-2)^{12}(-2)^{12}(-2)^{12}(-2)^{2} \\ &\equiv (1)(1)(1)(1)(4) \\ &\equiv 4 \pmod{13} \end{aligned}$$

Therefore, the remainder of 50^{50} on division by 13 is 4.

3.12 Product groups

Definition 3.20. Suppose that A and B are sets. The product of A and B is defined to be the set

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Thus an element of $A \times B$ is an ordered pair (a, b), where a is an element of A and b is an element of B.

Proposition 31. If G and H are groups, then $G \times H$ is a group under the binary operation defined as

$$(g, h) * (g', h') = (g *_G g', h *_H h').$$

3.13 Homomorphism

Definition 3.21. Let $(G, *_G)$ and $(H, *_H)$ be groups. A function $\phi : G \to H$ is a **homomorphism** (of **groups**) if

$$\phi(g *_G g') = \phi(g) *_H \phi(g') \quad \forall g, g' \in G.$$

Proposition 32. If $\phi : G \to H$ is a homomorphism of groups, then

1. $\phi(e_G) = e_H$;

2. $\phi(g^{-1}) = (\phi(g))^{-1}$.

Proposition 33. Suppose $\phi : G \to H$ is a homomorphism of groups. If $g \in G$ and $n \in \mathbb{Z}$, then $\phi(g)^n = \phi(g^n)$.

Proposition 34. Suppose that G, H and K are groups, and that $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms. Then $\psi \circ \phi : G \to K$ is a homomorphism.

Definition 3.22. If G and H are groups, then a function $\phi : G \to H$ is an **isomorphism** if it is a bijective homomorphism.

Proposition 35. Suppose that $G, H$and K are groups, and that $\phi : G \to H$ and $\psi : H \to K$ are isomorphisms. Then $\psi \circ \phi : G \to K$ is an isomorphism.

Proposition 36. Suppose that G and H are groups and $\phi : G \to H$ is an isomorphism. Let $\psi = \phi^{-1} : H \to G$ be the inverse function of ϕ. Then ψ is an isomorphism.

Definition 3.23. If G and H are groups, then we say G is **isomorphic** to H if there is an isomorphism $\phi : G \to H$.

Proposition 37. If $\phi : G \to H$ is a homomorphism, and g is an element of G of finite order, then the order of $\phi(g)$ divides the order g. If ϕ is injective, then the order of $\phi(g)$ is equal to the order of g.

Proposition 38. Suppose that G is a cyclic group.

1. If G has infinite order, then G is isomorphic to $\mathbb{Z}$.

2. If G has order n, then G is isomorphic to $\mathbb{Z}_n$.

Corollary 3.7.1. *If G is a group of prime order p, then G is isomorphic to $\mathbb{Z}_p$.*

Proposition 39. Suppose that G and H are isomorphic groups. Then

1. G is abelian if and only if H is abelian;

2. G is cyclic if and only if H is cyclic.

Proposition 40. Suppose that G and H are groups and $\phi : G \to H$ is an isomorphism. Then for each $g \in G$, the order of g in G is the same as the order of $\phi(g)$ in H.

Definition 3.24. The **image** of ϕ is defined as

$$\phi(G) = \{\phi(g) : g \in G\},$$

also denoted image(ϕ).

Proposition 41. Suppose that G and H are groups and $\phi : G \to H$ is a homomorphism. Then $\phi(G)$ is a subgroup of H.

Definition 3.25. Suppose that $\phi : G \to H$ is a homomorphism of groups. The **kernel** of ϕ is the following subset of G :

$$\ker(\phi) = \{g \in G : \phi(g) = e_H\}.$$

Proposition 42. Suppose that G and H are groups and $\phi : G \to H$ is a homomorphism. Then $\ker(\phi)$ is a subgroup of G.

4 Rings

Definition 4.1. A **ring** is a set R with binary operations $+$ and $*$ satisfying:

1. $(R, +)$ is an abelian group;
2. the operation $*$ is associative and has an identity elements in R;
3. $x * (y + z) = (x * y) + (x * z)$ and $(y + z) * x = (y * x) + (z * x)$ for all $x, y, z \in R$.

Example.

- $(\mathbb{Z}, +, \cdot)$;
- $(\mathbb{Q}, +, \cdot)$;
- $(\mathbb{R}, +, \cdot)$;
- $(\mathbb{C}, +, \cdot)$;
- $(\mathbb{Z}_n, +, \cdot)$;
- $(M_2(\mathbb{R}), +, \cdot)$.

4.1 Basic properties of rings

We will use 0_R to represent the **additive identity** and 1_R for **multiplicative identity.**

Proposition 43. Suppose that $(R, +, *)$ is a ring.

1. $0_R * x = 0 = x * 0_R$ for all $x \in R$.
2. $(-x) * y = -xy = x * (-y)$ for all $x, y \in R$.

Proposition 44. If $(R, +, \cdot)$ is a ring, then

$$(n \cdot x)y = n \cdot (xy) = x(n \cdot y)$$

for all $x, y \in R$ and $n \in \mathbb{Z}$.

Let m_R represent the m^{th} multiple of 1_R i.e. $m_R = m \cdot 1_R$.

Proposition 45. Suppose that R is a ring. Then

1. $m_R x = m \cdot x = x m_R$ for all $m \in \mathbb{Z}, x \in R$;
2. $m_R + n_R = (m + n)_R$ and $m_R n_R = (mn)_R$ for all $m, n \in \mathbb{Z}$;
3. $(m_R)^n = (m^n)_R$ for all $m \in \mathbb{Z}, n \in \mathbb{N}$.

4.2 Subring

Definition 4.2. Suppose that $(R, +, *)$ is a ring and S is a subset of R. Then S is a **subring** of R if S, with the operations $+$ and $*$, is a ring and $1_S = 1_R$.

Proposition 46. Suppose that $(R, +, *)$ is a ring and $S \subset R$. Then S is a subring of R if and only if all of the following hold:

1. $0_R \in S$ and $1_R \in S$;
2. if $x, y \in S$, then $x + y \in S$ and $x * y \in S$;
3. if $x \in S$, then $-x \in S$.

Definition 4.3. Suppose that $(R, +, *)$ is a ring. An element $x \in R$ is called a **unit** in R if x has a multiplicative inverse in R, i.e., if there exists an element $y \in R$ such that

$$x * y = 1_R = y * x.$$

Theorem 4.1. Suppose that $(R, +, *)$ is a ring. Then $(R^\times, *)$ is a group.

Remark. *For any ring R we let $R^\times$ denote the set of units in R.*

4.3 Types of rings

Definition 4.4. We say that a ring $(R, +, *)$ is **commutative** if the operation $*$ on R is commutative, i.e.

$$x * y = y * x \quad \text{for all } x, y \in R.$$

Definition 4.5. We say that a ring R is an **integral domain** (or simply a **domain**) if R is commutative, $0_R \neq 1_R$ and

$$x, y \in R, xy = 0_R \Rightarrow x = 0_R \text{ or } y = 0_R.$$

Proposition 47. Let n be a positive integer. Then $\mathbb{Z}_n$ is a domain if and only if n is prime.

Proposition 48. Suppose that R is an integral domain, $x, y, z \in R$ and $x = 0_R$. If $xy = xz$, then $y = z$.

Definition 4.6. A ring R is called a **field** if R is an integral domain and every non-zero element of R is a unit (where non-zero means different from 0_R).

Proposition 49. Suppose that R is a commutative ring. Then R is a field if and only if

$$R^\times = R \backslash \{0_R\} = \{x \in R : x \neq 0_R\}.$$

4.4 Matrix rings

Proposition 50. If R is a ring, then $M_n(R)$ is a ring under matrix addition and multiplication.

4.5 Ring homomorphism

Definition 4.7. Suppose that $(R, +_R, *_R)$ and $(S, +_S, *_S)$ are rings. A function $\phi : R \to S$ is a **homomorphism** (of **rings**) if all of the following hold:

1. $\phi(x +_R y) = \phi(x) +_S \phi(y)$ for all $x, y \in R$;
2. $\phi(x *_R y) = \phi(x) *_S \phi(y)$ for all $x, y \in R$;
3. $\phi(1_R) = 1_S$.

Proposition 51. Suppose that $\phi : R \to S$ is a homomorphism of rings. Then $\phi(n_R) = n_S$ for all $n \in \mathbb{Z}$.

Proposition 52. (This is from 2017 past paper.) Proposition 33 can be extended to homomorphism of rings with additive property: if $\phi : R \to S$ is a homomorphism of rings $r \in R$ and $n \in \mathbb{Z}$ then $\phi(n \cdot r) = n \cdot \phi(r)$.

Proposition 53. If $\phi : R \to S$ and $\psi : S \to T$ are homomorphisms of rings, then so is $\psi \circ \phi : R \to T$.

Proposition 54. Suppose that $\phi : R \to S$ is a homomorphism of rings. Then the restriction of ϕ defines a homomorphism of groups from $R^\times$ to $S^\times$. (In particular, if $r \in R^\times$, then $\phi(r) \in S^\times$.)

Example.

- The function $f : \mathbb{Z} \to \mathbb{Z}_n$, defined by $f(a) = [a]_n$;
- The complex conjugation $\mathbb{C} \to \mathbb{C}$ is a ring homomorphism;
- If R and S are rings, the zero function from R to S is a ring homomorphism if and only if S is the zero ring.

Remark. *There is **NO** ring homomorphism between $\mathbb{Z}_n \to \mathbb{Z}$ for $n \geq 1$.*

Definition 4.8. If R and S are rings, then a function $\phi : R \to S$ is called an **isomorphism** (of **rings**) if ϕ is a bijective homomorphism (of rings). In that case we say R is **isomorphic** to S.

Example. We have that $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Proposition 55. Suppose that $\phi : R \to S$ is an isomorphism of rings.

1. The inverse function $\phi^{-1} : S \to R$ is also an isomorphism of rings.
2. If $\psi : S \to T$ is also an isomorphism of rings, then so is the composite $\psi \circ \phi : R \to T$.

Corollary 4.1.1. *If $\phi : R \to S$ is an isomorphism of groups, then its restriction $R^\times \to S^\times$ is an isomorphism of groups.*

4.6 The Chinese Remainder Theorem

Theorem 4.2. If m and n are relatively prime positive integers, then the function

$$\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

defined by $\psi([a]_{mn}) = ([a]_m, [a]_n)$ is an isomorphism of rings.

Theorem 4.3. (The Chinese Remainder Theorem). Suppose that $a, b, m, n \in \mathbb{Z}$ with $m, n > 0$. If m and n are relatively prime, then there are integers $x \in Z$ which simultaneously satisfy the congruences

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}.$$

Theorem 4.3 does not explicitly outline how to find a solution to $[x]_{mn}$ in practice. This is done as follows: we use the Euclidean algorithm to find $r, s \in \mathbb{Z}$ such that $mr + ns = 1$. We note that

$$\begin{aligned} mr &\equiv 0 \pmod{m}, \quad mr \equiv 1 \pmod{n} \\ ns &\equiv 1 \pmod{m}, \quad ns \equiv 0 \pmod{n}. \end{aligned}$$

Therefore letting $x_0 = b(mr) + a(ns)$ gives

$$\begin{aligned} x_0 &\equiv b \cdot 0 + a \cdot 1 \equiv a \pmod{m} \\ \text{and } x_0 &\equiv b \cdot 1 + a \cdot 0 \equiv \pmod{n}. \end{aligned}$$

Therefore the general solution is $x \equiv bmr + ans \pmod{mn}$.

Remark. *To solve system of congruence with 3 or more congruences, solve a pair with the Chinese remainder theorem first. Then use the the result to solve the next pair and vice versa.*

Example. Use the Chinese Remainder Theorem to find all integers x such that

$$x \equiv 11 \pmod{47} \quad \text{and} \quad x \equiv 3 \pmod{31}.$$

Solution:
First we check if 47 and 31 are relatively prime. They are since $\gcd(47, 31) = 1$.

We use the Euclidean Algorithm to solve find $r, s \in \mathbb{Z}$ such that $47r + 31s = 1$. We begin as such:

$$\begin{aligned} 47 &= 1 \cdot 31 + 16 \\ 31 &= 1 \cdot 16 + 15 \\ 16 &= 1 \cdot 15 + 1 \end{aligned}$$

We can "unwind" the system of equations:

$$\begin{aligned} 1 &= 16 - 15 \\ &= 16 - (31 - 16) \\ &= 2 \cdot 16 - 31 \\ &= 2(47 - 31) - 31 \\ &= 2 \cdot 47 - 3 \cdot 31 \end{aligned}$$

Therefore we have that $r = 2$ and $s = -3$. The general solution of the system of congruences

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}$$

is given by

$$x \equiv bmr + ans \pmod{mn}.$$

Hence, the solution to our system of congruences is:

$$\begin{aligned} &x \equiv (3)(47)(2) + (11)(31)(-3) \pmod{47 \times 31} \\ &x \equiv 282 - 1023 \pmod{47 \times 31} \\ &x \equiv -741 \pmod{47 \times 31} \\ &x \equiv 716 \pmod{47 \times 31} \end{aligned}$$

This means that,

$$\begin{aligned} x - 716 &= 1457k \\ x &= 716 + 1457k \quad \text{for } k \in \mathbb{Z}. \end{aligned}$$

Example. Use the Chinese Remainder Theorem to find all integers x such that

$$4x \equiv 5 \pmod{9} \quad \text{and} \quad 2x \equiv 6 \pmod{20}.$$

Solution:
We begin by finding the a solution for each system of congruence independently i.e. find a solution of x for $4x \equiv 5 \pmod{9}$ and $2x \equiv 6 \pmod{20}$. By using the Euclidean Algorithm we find that

$$x \equiv 9 \pmod{9} \quad \text{and} \quad x \equiv 3 \pmod{10}.$$

Then we can use the Chinese Remainder Theorem as in the example above.

4.7 Euler's φ function

Definition 4.9. Euler's φ function (or **Euler's totient function**) is the number of integers in $\{0, 1, 2, \ldots, n-1\}$ which are relatively prime to n.

Proposition 56. If $n = p$ where p is prime then $\varphi(p) = p - 1$.

Proposition 57. If $n = p$ where p is prime then $\varphi(p^r) = p^r - p^{r-1} = (p-1)p^{r-1}$.

Corollary 4.3.1. *If m and n are relatively prime, then $\mathbb{Z}_{mn}^{\times}$ is isomorphic to $\mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$. In particular, if* $\gcd(m,n) = 1$, *then* $\varphi(mn) = \varphi(m)\varphi(n)$.

Example. $\varphi(300) = \varphi(2^2 \times 3 \times 5^2) = \varphi(2^2)\varphi(3)\varphi(5^2)$.

Corollary 4.3.2. *Suppose that n is a positive integer and a is an integer relatively prime to n. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$