Algebra 1H

typed up by B. S. H. Mithrandir

- *Last compiled: May 2021*
- Adapted from notes of N. Martin, Durham
- This was part of the Durham Core A module given in the first year. This is an introduction to group theory, number theory, and proofs.

- **TODO!** diagrams

1 Groups and numbers

A **group** G is a non-empty set with structure coming from a **binary group operation**, usually denotes $\circ$. For every pair $g_1, g_2 \in G$, there exists $g_1 \circ g_2$ (g_1 is **composed** with g_2). To be a group, the following conditions needs to be satisfied:

1. **Closure**: for all $g_1, g_2 \in G$, $g_1 \circ g_2 \in G$.

2. **Associativity**: for all $g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

3. **Identity**: There exists $e \in G$ such that, for all $g \in G$, $e \circ g = g \circ e = g$.

4. **Inverse**: There exists $g_i^{-1} \in G$ such that, for all $g_i \in G$, $g_i^{-1} \circ g_i = g_i \circ g_i^{-1} = e$, and $g_i^{-1} \neq g_j^{-1}$ if $i \neq j$.

Example 1. Let $\mathsf{M}(m, n, \mathbb{R})$ be an $m \times n$ matrix with real coefficients. Under matrix multiplication, it is a group is $m = n$ and $|\mathbb{M}| \neq 0$; this is called the **general linear group** $\mathrm{GL}(n, \mathbb{R})$. Note this group is not commutative (the ordering of composition matters).

2. $C_n = \{\exp(2k\pi\mathrm{i}/n) \mid 0 \leq k \leq n-1\}$ is a group under multiplication: $1 = \mathrm{e}^{2\pi\mathrm{i}}$ is the identity element, and it is closed if we remove the excess multiples of $\mathrm{e}^{2\pi\mathrm{i}}$. With this, the inverse is easily defined, and it is associative by properties of multiplication. This is the **cyclic** group of n elements, with $\exp(2\pi\mathrm{i}/n)$ being the **generator** (more later).

3. $G = \{-1, 1\}$ under multiplication and $H = \{\text{even}, \text{odd}\}$ under addition of numbers are both groups. In particular, there is a one-to-one identification between $1 \leftrightarrow$ even and $-1 \leftrightarrow$ odd, so the two groups have similar structure. G is actually **isomorphic** to H, denoted $G \cong H$.

4. A non-square rectangle has the symmetries $\{I, H, V, R\}$ which are, respectively, the identity (i.e., doing nothing), horizontal reflection, vertical reflection, and rotation by π. A group table may be formed (row first, then column). Contrast this with $C_4 = \{1, -1, \mathrm{i}, -\mathrm{i}\}$ under multiplication: The two have different structures, so are not

$\circ$	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

$\times$	1	-1	i	$-\mathrm{i}$
1	1	-1	i	$-\mathrm{i}$
-1	-1	1	$-\mathrm{i}$	i
i	i	$-\mathrm{i}$	-1	1
$-\mathrm{i}$	$-\mathrm{i}$	i	1	-1

isomorphic.

Lemma 1.0.1 *The identity and the inverse in a group is unique.*

Proof Suppose $e, f \in G$ are identity elements, then

$$ef = e, \qquad ef = f \qquad \Rightarrow \qquad e = f,$$

so we have uniqueness. Suppose h and k are both inverses to g, then

$$h = he = h(gk) = (hg)k = ek = k,$$

so we also have uniqueness. ■

1.1 Numbers

Theorem 1.1.1 *Let $n, m \in \mathbb{Z}$, $m > 0$. There exists $q, r \in \mathbb{Z}$ such that $n = qm + r$, $0 \leq r < n$. (Here, q is quotient, r is remainder.)* □

We say m divides n ($m|n$) is there exists q such that $n = mq$, i.e., $r = 0$.

Lemma 1.1.2 *1. For all n, $n|0$.*

2. For all n, $n|1$.

3. For all n, $n|n$.

4. $l|m$ and $m|n$ implies $l|n$.

5. If $n \neq 0$, $0 \nmid n$.

6. $n|a$ and $n|b$ implies that $n|(a \pm b)$. □

Prime numbers have exactly two distinct factors (so 1 is not prime).

Lemma 1.1.3 *If n is not prime, there exists a prime $p \leq \sqrt{n}$ such that $p|n$.*

Proof If n is not prime, then there are at least three factors, and every such divisor is less than or equation to n. Let $p > 1$ be the smallest divisor of n. p is prime because if there is a k where $k|p$, then $k|p|n$ and p is not the smallest divisor of n. $p|n$ so $n = pq$, thus $p \leq \sqrt{n}$, otherwise q would be a smaller non-trivial factor of n. ■

Theorem 1.1.4 (Fundamental theorem of arithmetic) *Let $n \in \mathbb{Z}$, $|n| > 1$. It is possible to write*

$$n = \pm p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

where $k \geq 1$, $p_1 < p_2 < \cdots < p_k$ are prime numbers, and, for all $i \in \mathbb{N}$, $r_i \geq 1$, i.e., all integers may be written as a product of prime numbers. □

Theorem 1.1.5 *There are infinite many prime numbers.*

Proof We carry out a proof by contradiction. Suppose there are finite number of primes with $0 < p_1 < p_2 < \cdots < p_k$. Let $n = p_1 p_2 \cdots p_k + 1$. For all i, diving by p_i gives remainder 1. However, the fundamental theorem of arithmetic guarantees n may be factorised as primes, therefore the list above is not complete. ■

1.1.1 *Common factors*

Example The numbers 336 and 231 have the greatest common divisor (gcd) of 21:

$$336 = 231 + 105, \qquad 231 = 2 \times 105 + 21, \qquad 105 = 5 \times 21 + 0.$$

We write $\gcd(336, 231) = 21$.

Here, we can define an algorithm that generates the gcd of any two integers.

Proposition 1.1.6 (Euclidean algorithm) *Given $m, n \in \mathbb{Z}^+$, the following algorithm generates gcd(m,n):*

1. *If $m > n$, swap so $n > m$;*

2. *$n = q \cdot m + r$, $0 \leq r < m$;*

3. *If $r = 0$, output m as gcd and stop;*

4. *Otherwise, replace $n = m$, $m = r$, and repeat from step 2.* □

Theorem 1.1.7 *Euclidean algorithm generates $\gcd(m, n)$.*

Proof Let d be any common divisor, then $d|m$ and $d|n$, and thus $d|(n - qm) = r$. At each stage the same divisor divides each m, n and r until $r = 0$, and current value of m is our output number, the gcd. ■

Corollary 1.1.8 *Given any $m, n \in \mathbb{Z}^+$ with $\gcd(m, n) = d$, we can always write $d = mx + ny$ for $x, y \in \mathbb{Z}$.*

Proof At each step of the Euclidean algorithm, we can write the current values of m, n and r as a linear combination of the original values. The k^{th} step of the iteration makes us solve

$$n_k = q_k m_k + r_k \qquad \Leftrightarrow r_k = n_k - q_k m_k.$$

For all k, r_k is a linear combination in the cycle of iterations. Process starts with original m, n and ends with the gcd in the form of a linear combination. ■

Example $21 = \gcd(336, 231)$. We have

- $336 = 231 + 105$, $105 = 336 - 231$.
- $231 = 2 \times 105 + 21$, $21 = 231 - 2(336 - 331) = 3 \times 231 - 2 \times 336$.

1.1.2 *Modular arithmetic*

Theorem 1.1.9 *There are infinitely many primes of the form* $4k + 3$.

Proof Suppose this is false, then there is a largest prime n, $n \geq 3$. Let $N = (4n)! - 1 = 4m - 1$, $m \in \mathbb{Z}$. By the fundamental theorem of arithmetic, since $(4m - 1)$ is odd, we see all primes involved are odd. Everyone of our original list of primes of the form $4k + 3$ gives remainder -1 when divided into N, so none of these are factors.

All factors of N thus have the form $4\ell + 1$, $\ell \in \mathbb{Z}$. All products of $4\ell + 1$ results in a number $4\ell' + 1$ which is a contraction to the statement that prime products have the form $4m - 1$. ■

For $n \in \mathbb{Z}$, $a, b \in \mathbb{Z}$ are **congruent modulo** n if $n|(a - b)$, denoted $a \equiv b \pmod{n}$. Since $a \equiv b \pmod{n}$ iff $a = b + nk$ for $k \in \mathbb{Z}$. We see this may also define an equivalence relation.

Example

$$27 \equiv 2 \pmod{5}, \quad 101 \equiv 24 \pmod{11},$$
$$-37 \equiv 53 \pmod{1}, \quad 10^n - 1 \equiv 0 \pmod{9}.$$

The **congruence class of** a **mod** n is defined to be $\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}$.

Example The congruence class of 0 mod 5 and 1 mod 5 are respectively

$$\overline{0} = \{\cdots, -5, 0, 5, \cdots\}, \qquad \overline{1} = \{\cdots, -4, 1, 4, \cdots\}.$$

There are only five distinct congruence classes in mod 5, represented by the **principal residues** in the range $\overline{0}, \cdots \overline{4}$. In general, for $n \in$

$\mathbb{Z}$, there are n distinct congruence classes mod n, represented by $\overline{0}, \overline{1}, \cdots \overline{n-1}$.

For general n, we take the set of integer mod n as $\mathbb{Z}_n$ (or $\mathbb{Z}_n/\mathbb{Z}$). We can sometimes solve $ax \equiv b \pmod{n}$ for x. For example, $7x \equiv 14 \pmod{35}$ may be reduced to $x \equiv 2 \pmod{5}$, and so $x = 2 + 5n \in \mathbb{Z}_{35}$. However, we see $7x \equiv 15 \pmod{35}$ cannot be solved for $x \in \mathbb{Z}$ since $7 \nmid 15$, but $7 | 14$ and $7 | 35$.

Proposition 1.1.10 *$\mathbb{Z}_n$ is a group under addition. $\overline{0}$ acts like zero, we have closure, associativity from addition, and the inverse of $\overline{a}$ is given by $\overline{n-a}$.* □

In addition, $\mathbb{Z}_n$ is a cyclic group with generator $\overline{1}$.

Proposition 1.1.11 *Let p be prime, $\overline{a} \neq \overline{0} \in \mathbb{Z}_p$, then:*

- *there exists $\overline{b}$ such that $\overline{a} \times \overline{b} = \overline{1}$;*
- *for all $\overline{c} \in \mathbb{Z}_p$, there exists $\overline{x}$ such that $\overline{a} \times \overline{x} = \overline{c}$;*
- *$\mathbb{Z}_p - \{\overline{0}\}$ is a group under multiplication.*

Proof
- If p is prime and $a \neq 0 \pmod{p}$, then $\gcd(a, p) = 1$. So there exists b and c such that $ab + pc = 1$, but
$$1 = ab + pc \equiv ab \pmod{p},$$
so $\overline{a} \times \overline{b} = \overline{1}$ in $\mathbb{Z}_p$ with $b \neq 0$.
- From the previous part, $\overline{c} = \overline{c}\overline{1} = \overline{c}(\overline{a}\overline{b}) = \overline{a}(\overline{c}\overline{b})$. Let $\overline{x} = \overline{c}\overline{b}$, and we have the result.
- Associativity is trivial. $\overline{1}$ is the identity, and we proved existence of the inverse in the previous parts. ■

Lemma 1.1.12 *Let $0 < a < n$, $a, n \in \mathbb{Z}$, $\gcd(a, n) = 1$. Then there exists b with $0 < b < n$ such that $ab \equiv 1 \pmod{n}$.*

Proof $\gcd(a, n) = 1$ implies that we have $ax + ny = 1$ for some $x, y \in \mathbb{Z}$. Select a b such that $b \equiv x \pmod{n}$ implies that $ab \equiv ax = 1 - ny \equiv 1 \pmod{n}$.

Suppose b is not unique, and b' also exists. Working in mod n,
$$\overline{b'} = \overline{b'} \cdot \overline{1} = \overline{b'}(\overline{a}\overline{b}) = (\overline{b'}\overline{a})\overline{b} = \overline{1} \cdot \overline{b} = \overline{b},$$
so $\overline{b}$ is unique. ■

Two numbers a and b are **co-prime** if $\gcd(a, b) = 1$.

$\mathbb{Z}_n - \{0\}$ is not generally a group under multiplication. Let $n \geq 2$, $n \in \mathbb{Z}$, then we define
$$\mathbb{Z}_n^* = \{\overline{r} \mid 1 \leq r \leq n,\ \gcd(r, n) = 1\}.$$

We observe that $\mathbb{Z}_n^* \subseteq \mathbb{Z}_n$. We have, for example,

$$\mathbb{Z}_3^* = \{\overline{1}, \overline{2}\}, \qquad \mathbb{Z}_4^* = \{\overline{1}, \overline{3}\}, \qquad \mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}.$$

Proposition 1.1.13 *We have that:*

1. *$\mathbb{Z}_n^*$ is well defined;*
2. *$\mathbb{Z}_n^*$ is closed under multiplication;*
3. *the inverse of a residue is also in $\mathbb{Z}_n^*$;*
4. *if $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n^*$, with $\overline{ab} = \overline{ac}$, then $\overline{b} = \overline{c}$;*
5. *$\mathbb{Z}_n^*$ is a group under multiplication.*

Proof In order:

1. We see a residue is represented by all others that are congruent to it. However, if k is a number, $k \equiv x \pmod{n}$, then $x = k + tn$, $t \in \mathbb{Z}$. So $\gcd(k, n) = 1$ iff $\gcd(x, n) = 1$, so $\mathbb{Z}_n^*$ is well defined.
2. $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ implies that $\gcd(ab, n) = 1$, so we have closure.
3. There exists x and y where $ax + ny = 1$, so $\gcd(ax, n) = 1$, which implies $\gcd(x, n) = 1$, and so inverse exists and belongs to $\mathbb{Z}_n^*$ from the previous point.
4. Let x be the inverse residue, then
$$\overline{xab} = \overline{xac} \qquad \Rightarrow \qquad \overline{1b} = \overline{1c},$$
and $\overline{b} = \overline{c}$.
5. We have proved this from the above points. ■

Theorem 1.1.14 *In modulo n, $n \geq 2$, let $a > 0$, $c \geq 0$, $a, c \in \mathbb{Z}$:*

1. *if $\gcd(a, n) = 1$, there exists x with $0 \leq x < n$ where $ax \equiv c \pmod{n}$, and x is unique;*
2. *if $\gcd(a, n) = d > 1$ and $d \nmid c$, then there is no x where $ax \equiv c \pmod{n}$;*
3. *if $\gcd(a, n) = d > 1$ and $d | c$, there are d values of x, $0 \leq x < n$ such that $ax \equiv c \pmod{n}$.*

Proof As follows:

1. If $\gcd(a, n) = 1$ and, then $\overline{a} \in \mathbb{Z}_n^*$, so there exists $\overline{y} \in \mathbb{Z}_n^*$ such that $\overline{ay} = 1$. Let x be the residue of yc in mod n, then we get
$$ax = (ay)c \equiv 1 \cdot c = c \pmod{n},$$
so x exists. Suppose x' is another such residue, then $ax - ax' \equiv 0 \pmod{n}$, and so
$$x - x' \equiv 1 \cdot (x - x') \equiv ya(x - x') = y(ax - ax') \equiv 0 \pmod{n}.$$

2. $ax \equiv c \pmod{n}$ implies that $ax = c + kn$ for some k. Thus $c = ax - kn$, and $\gcd(a, n) = d$ necessarily implies that $d|c$, so we have a contradiction.

3. Here, there exists $b, e, m \in \mathbb{Z}$ such that $a = bd$, $c = ed$ and $n = md$. We have $\gcd(b, m) = 1$, and so by (i) there exists an unique t with $0 \leq t < m$ such that $bt = e \pmod{m}$. The claim is that $x = t + rm$ with $0 \leq r \leq d - 1$ are the d solutions to the original equation $ax \equiv \pmod{n}$. This is because

$$a(t + rm) = bd(t + rm) = d(bt) + br(dm),$$

and since $bt \equiv c \pmod{m}$, this implies that

$$d(bt) + br(dm) = d(e + km) + brn = de + k(dm) + brn = c + kn + brn = c + (k + br)n.$$

Indeed, $x + t + rm$ are the solutions to $ax \equiv c \pmod{n}$.

If x and x' are distinct solutions, then $a(x - x') \equiv 0 \pmod{n}$, and $a(x - x') = kn$. This means that we have $db(x - x') = kdm$, thus $b(x - x') = km$, and so $b(x - x') = 0 \pmod{n}$. Hence

$$\gcd(b, m) = 1 \qquad \Rightarrow \qquad x - x' \equiv 0 \pmod{m}$$

as required. ■

Example 1. $9x \equiv 8 \pmod{23}$. We have $\gcd(9, 23) = 1$, and we see that $1 = 2 \cdot 23 - 5 \cdot 9$, so $-5 \cdot 9 \equiv 1 \pmod{23}$; thus

$$x \equiv (-5 \cdot 9)x \equiv -5 \cdot (9x) \equiv -5 \cdot 8 \equiv -40 \equiv 6 \pmod{23}.$$

2. $10x \equiv 14 \pmod{18}$. Now, $\gcd(10, 18) = 2$, and we see that $10x = 14 + 18k$ is equivalent to $5x = 7 + 9k$, and now we have $5x \equiv 7 \pmod{9}$ and $\gcd(5, 7) = 1$. Since $1 = 2 \cdot 5 - 1 \cdot 9$, $2 \cdot 5 \equiv 1 \pmod{9}$, and

$$x \equiv (2 \cdot 5)x \equiv 2 \cdot 7 \equiv 14 \equiv 5 \pmod{9}.$$

By the theorem, there should be two distinct values of x, and so $x = 5, 14$.

3. $25x \equiv 65 \pmod{90}$. Here, $\gcd(25, 90) = 5$, and diving through by 5 gives $5x = 13 + 18k$, and now $5x \equiv 13 \pmod{18}$, $\gcd(5, 13) = 1$, with $1 = 2 \cdot 18 - 7 \cdot 5$. Thus

$$x \equiv (-7 \cdot 5)x \equiv -7 \cdot 13 \equiv -91 \equiv 17 \pmod{18},$$

with $x = 17, 35, 53, 71, 89$.

4. $20x \equiv 65 \pmod{90}$. Here, $\gcd(20, 10) = 10$, however, $10 \nmid 65$, so there are no solutions in $\mathbb{Z}$.

Corollary 1.1.15 (Chinese remainder theorem) *Suppose* $gcd(m, n) = 1$, $0 \leq a < m$ *and* $0 \leq b < n$. *Then there exists an unique* c *with* $0 \leq c < mn$ *such that* $c \equiv a \pmod{m}$ *and* $c \equiv b \pmod{n}$.

Proof We need $c = a + km$ and $c = b + ln$. Thus $km = c - a \equiv b - a \pmod{n}$. Now, $\gcd(m, n) = 1$, so there exists x and y such that $mx + ny = 1$. Choosing $c = a + x(b-a)m$ gives $c \equiv a \pmod{m}$. Now, $mx = 1 - ny$ gives

$$c = a + (b-a)(1-my) = b + y(a-b)n,$$

so $c \equiv b \pmod{n}$ also. ■

Example With $c \equiv 6 \pmod{8}$ and $c \equiv 13 \pmod{15}$, we have $0 \leq c < 8 \cdot 15 = 120$, and noticing $2 \cdot 8 - 1 \cdot 15 = 1$, we have $x = 2$, and $c = 6 + 2(13-6)8 = 118$.

1.1.3 *Totient function*

Let the number of elements in $\mathbb{Z}_n^*$ be denoted by $\phi(n)$, the **Euler ϕ-function**, also called the **totient function**. For $n \geq 3$, $\phi(n)$ is always even, while for p prime, $\phi(p) = p - 1$, and $\phi(p^n) = p^n - p^{n-1}$. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Theorem 1.1.16 (Euler–Fermat theorem) *Let* $n > 1$, $gcd(a, n) = 1$. *Then* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof Let $[\overline{x_1}, \overline{x_2}, \cdots, \overline{x_{\phi(n)}}]$ be a list of all distinct elements of $\mathbb{Z}_n^*$. Let $z = \prod_{i=1}^{\phi(n)} \overline{x_i}$. Now consider $[a\overline{x_1}, a\overline{x_2}, \cdots, a\overline{x_{\phi(n)}}]$. By proposition, all elements are distinct, and all elements are in $\mathbb{Z}_n^*$, i.e., the list is a permutation of the original list. Thus

$$\overline{z} = \prod_{i=1}^{\phi(n)} (a\overline{x_i}) = a^{\phi(n)}\overline{z},$$

so $1 \equiv a^{\phi(n)} \pmod{n}$. ■

Example: public key cryptography This above idea is used in public key cryptography. The idea is that Alice sends Bob a secure message T. Bob has a public method of encoding the message (the **public key**). Alice encodes T to M and sends this to Bob. Bob has a secret way to decode M to recover T.

Bob chooses two very large and distinct prime numbers p and q. He also chooses two very large numbers d and e such that

$$de \equiv 1 \pmod{(p-1)q-1)}.$$

Bob makes e public.

Alice converts her message into numbers all less than p and q. Let T be one such number. Alice works out the residue $M \equiv T^e \pmod{pq}$ and sends M. Bob works out the residue $U \equiv M^d = (T^e)^d$, and $U = T$. To show this, we observe that, since $T < q$ and $T < p$, $\gcd(T, pq) = 1$. By the Euler–Fermat theorem, $T^{\phi(pq)} \equiv 1 \pmod{pq}$. Since p and q are co-prime,

$$\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

Bob chooses $ed \equiv 1 \pmod{(p-1)(q-1) = \phi(pq)}$, so

$$ed = k\phi(pq) + 1, \qquad k \in \mathbb{Z}.$$

Thus

$$(T^e)^d = T^{k\phi(pq)+1} = T^{k\phi(pq)}T = [T^\phi(pq)]^k T \equiv 1^k \cdot T = T \pmod{pq}.$$

As an example, consider $p = 7, q = 13$. Then $pq = 91$, and $\phi(pq) = (7-1)(13-1) = 72$. We need e and d to be co-prime to 72, and mutually inverse in $\mathbb{Z}_{72}^*$; we observe that $e = 5$ and $d = 79$ works. Suppose $T = 10$ is the thing we are sending; observe that $\gcd(10, 7) = \gcd(10, 13) = 1$.

To encode, we have $T^e = 10^5 = 1098 \cdot 91 + 82 \equiv 82 \pmod{91}$. To decode, $82^d = 82^29 \equiv 10 \pmod{91}$, as required.

Two groups G and H are **isomorphic**, $G \cong H$ if there is a mapping $\alpha : G \to H$ such that:

1. α is a **homomorphism**, i.e., $\alpha(g_1 \circ g_2) = \alpha(g_1) \circ \alpha(g_2)$;
2. α is bijective, i.e., injective and surjective.

If G and H are two groups, then the **Cartesian product** is defined to be

$$G \times H = \{(g, h) \mid g \in G,\ h \in H\}, \qquad (g_1, h_1) \circ (g_2, h_2) = (g_1 \circ g_2, h_1 \circ h_2).$$

With this, the identity element in $G \times H$ is (e_G, e_H), the inverse is $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Example For $\mathbb{Z}_m \times \mathbb{Z}_n$, with addition being the operation we have:

1. closure with $(\overline{a_1}, \overline{b_1}) + (\overline{a_2}, \overline{b_2}) = (\overline{a_1 + a_2}, \overline{b_1 + b_2})$;
2. associativity by inheritance;
3. identity is $(\overline{0}, \overline{0})$;
4. the inverse to $(\overline{a}, \overline{b})$ is $(-\overline{a}, -\overline{b})$.

So $\mathbb{Z}_m \times \mathbb{Z}_n$ is a group under addition, with $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$.

Theorem 1.1.17 *If m and n are co-prime, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.*

Proof Observe that $(\overline{1}, \overline{1}) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is the identity, corresponding to $\overline{1} \in \mathbb{Z}_{mn}$. We define

$$\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \qquad \phi(\overline{k}) = k(\overline{1}, \overline{1}) = (\overline{k}, \overline{k}).$$

(We will be calculating in the correct modulos are required.) Suppose $\phi(\overline{k}) = \phi(\overline{l})$, then $k \equiv l \pmod{m}$ and $k \equiv l \pmod{n}$. Thus $m|(k-l)$ and $n|(k-l)$, so $\gcd(m,n) = 1$, and hence $mn|(k-l)$, therefore $k \equiv l \pmod{mn}$. So we have preserved the algebraic structure, and ϕ is injective. Further, $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m n|$, so we have surjectivity.

Trivially, $\phi(\overline{k} + \overline{l}) = \phi(\overline{k}) + \phi(\overline{l})$ and $\phi(\overline{kl}) = \phi(\overline{k})\phi(\overline{l})$, so we have a homomorphism, and so $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_m n$ when m and n are co-prime. ■

If G is a finite group, and for all $g_1, g_2 \in G$, $g_1 \circ g_2 = g_2 \circ g_1$, G is called **abelian**, and is isomorphic to groups with form $\mathbb{Z}_n$.

Number of elements in group	Type
p prime	$\mathbb{Z}_p$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
6	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$
8	$\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$

Let G be a cyclic group, $g \in G$. The **order** of g is the least positive integer r such that $g^r = e$. If corresponding elements do not have the same order, then we do not have an isomorphism; the converse however is not true.

Example Consider the following examples:

1. $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, we observe that $\overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1}$, so $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
2. $\mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}$, and $\mathbb{Z}_9^* \cong \mathbb{Z}_6$ because it is the group with six elements.
3. $\mathbb{Z}_1 5^*$ has eight elements, and the order 2 elements are $\overline{4}, \overline{11}, \overline{14}$, whilst the order 4 elements are $\overline{2}, \overline{7}, \overline{8}, \overline{13}$, and it may be seen that $\mathbb{Z}_1 5^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

1.2 *Permutations*

A **permutation** is a re-arrangement of an order collection of objects. Consider the set $C_n = \{1, 2, \cdots n\}$. A permutation σ may be viewed as a bijective function σ from C_n to itself.

Proposition 1.2.1 *There are $n!$ distinct permutations of C_n.* □

In terms of notation, we write

$$\sigma = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{Bmatrix}$$

for $1 \mapsto 5$ etc. Things in he top row are mapped to the bottom row.

Let S_n be the set of permutations of C_n. We want S_n to be a group under composition of functions. Let $\sigma, \tau : C_n \to C_n$, be two permutations, then $\sigma\tau$ or $\tau\sigma$ is also a permutation.

Example For

$$\sigma = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{Bmatrix}, \qquad \tau = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{Bmatrix},$$

we have

$$\begin{aligned} \sigma\tau &= \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{Bmatrix} \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{Bmatrix} \\ &= \begin{Bmatrix} 2 & 3 & 4 & 5 & 1 \\ 4 & 3 & 2 & 1 & 5 \end{Bmatrix} \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{Bmatrix} \\ &= \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{Bmatrix}. \end{aligned}$$

This is **permutation multiplication**, by arranging top/bottom line accordingly.

Proposition 1.2.2 *S_n is a group under multiplication of permutations.*

Proof S_n is closed, composition of functions is associative, and the identity is the obvious one. We obtain the inverse permutation σ^{-1} by swapping the two rows of σ. ■

Consider S_3. $|S_3| = 3! = 6$, so it may be isomorphic to $\mathbb{Z}_6$. However, we notice that S_3 is non-abelian, so it is a distinct group class. In general, for $n \geq 3$, S_n is non-abelian.

1.2.1 Cycles

A **cycle** on a subset of C_n is a sequence $(a_1, a_2, \cdots a_k)$ of distinct elements of C_n, with $k \leq n$. This is a permutation where

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k - 1 \mapsto a_k \mapsto a_1, \qquad r \mapsto r$$

for other values now in the cycle. This is a ***k*-cycle**, denoted $(a_1 a_2 \cdots a_k)$, as it is made of k elements. Cycles can be written in several ways:

$$(a_1 a_2 \cdots a_k) = \cdots = (a_i a_{i+1} \cdots a_k a_1 \cdots a_{i-1}).$$

Two cycles are **disjoint** if they have no moving elements in common; for example, (2517) and (634) are disjoint, but (2517) and (654) are not.

Lemma 1.2.3 *If σ and τ are disjoint cycles, then $\sigma\tau = \tau\sigma$.*

Proof Moving distinct elements means order of permutation does not matter. ∎

Theorem 1.2.4 *Every permutation is an unique produce of disjoint cycles.*

Proof Let $\sigma : C_n \to C_n$ be a permutation. Choose $a \in \mathbb{Z}$, $1 \le a \le n$, and let $\sigma^i(a)$ be σ applied to a i times (so $\sigma^0(a) = a$). Consider the sequence

$$a,\ \sigma(a),\ \sigma^2(a),\ \cdots\ \sigma^i(a),\ \cdots.$$

C_n is finite, so sequence will eventually repeat itself, and there is a first time where $\sigma^r(a) = \sigma^s(a)$, with $r < s$. Suppose $r > 0$, then $\sigma(\sigma^{r-1}(a)) = \sigma(\sigma^{s-1}(a))$, but σ is bijective, which implies $\sigma^{r-1}(a) = \sigma^{s-1}(a)$; thus we have a contradiction, and $r = 0$.

Now, let

$$\gamma(a) = \left(a\ \sigma(a)\ \sigma^2(a)\ \cdots\ \sigma^{s-1}(a)\right)$$

be a cycle. We construct $\gamma_1 = \gamma(a_1)$, a cycle that starts with $a_1 = 1$. If $\gamma_1 = \sigma$, we have what we want, otherwise, there is a least number $a_2 \in \gamma_1$, and we construct $\gamma_2 = \gamma(a_2)$, a cycle starting with a_2. Now, γ_1 and γ_2 are disjoint by assumption; if $\gamma_1\gamma_2 = \sigma$ then we are done. Otherwise we repeat the process, and since C_n is fnite, there is a finite collection of k where $\gamma_1\gamma_2\cdots\gamma_k = \sigma$. This is essentially unique because whenever we have a number a, it is automatically in a cycle of its own. ∎

Example

$$\sigma = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 3 & 8 & 2 & 4 & 1 & 6 \end{Bmatrix} = (1527)(3)(486),$$

$$\tau = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 5 & 9 & 1 & 2 & 8 & 7 & 4 \end{Bmatrix} = (16235)(49)(78).$$

Usually trivial cycles are omitted, so $\sigma = (1527)(486)$.

Example To multiply cycles, consider $\sigma = (135)(48)$ and $\tau = (3218)(46)(57)$, then

$$\sigma\tau = (135)(48)(3218)(46)(57),$$

and sending 1 through from the right, we see that $1 \to 8 \to 4 \to 4$, and $4 \to 6 \to 6$, etc. Doing this for all numbers, we see that $\sigma\tau = (146857)(23)$.

Lemma 1.2.5 *Let $(a_1 \cdots a_k)$ be a k-cycle, then*

$$(a_1 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2),$$

and it is trivial to check this. □

A 2-cycle is called a **transposition**. From this, we can deduce the following:

Theorem 1.2.6 *Every permutation is a product of transpositions, which follows from the fact that each permutation is a product of disjoint cycles, and every cycle is a produce of transpositions.*

1.2.2 Cycle types

Every permutation is a product of disjoint cycles, $\sigma = \gamma_1 \cdots \gamma_r$, say. Suppose teh cycle γ_i has length k_i. The unordered sequence of numbers $k_1, k_2 \cdots k_r$ is the **cycle type** of σ. For example, $(123)(45)$ has type $(3, 2)$, and $(12)(34)(567)$ has type $3, 2, 3$.

Proposition 1.2.7 *A permutation of cycle type $k_1, \cdots k_r$ may be expressed as a product of $(k_1 + \cdots + k_r) - r$ transpositions.* □

The **parity** of this number $(k_1 + \cdots + k_r) - r$ is a property of the permutation.

Theorem 1.2.8 (Matrix determinants) *For a $n \times n$ matrix A,*

$$|\mathsf{A}| = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)},$$

where $\epsilon(\sigma)$ depends on the parity of the permutation σ. This is the real definition of the determinant of a matrix. □

Theorem 1.2.9 *Given a permutation σ written in two ways, one as a product of r transpositions, the other as a product of s transpositions, r and s will have the same parity.* □

The **order** of a permutation is the least amount of times the permutation is composed with itself to get back to the identity. A k-cycle has order k.

Theorem 1.2.10 *Let $\sigma = \gamma_1 \cdots \gamma_k$, γ_i disjoint from γ_j for $i \neq j$, and for each i, γ_i has length r_i. Then the order of σ is lcm$\{r_1, r_2, \cdots, r_k\}$.*

Proof Let $\sigma^t = \gamma_1^t \gamma_2^t \cdots \gamma_k^t$. For $\sigma^t = e$, $r_i | t$ for all i, and the lowest such t is the lowest common multiple of the un-ordered set $\{r_1, r_2, \cdots, r_k\}$. ■

1.3 More on groups

Here, we write group binary operation as $g \circ h = gh$.

1.3.1 *Subgroups*

A **subgroup** of a group G is a subset $H \subseteq G$ such that H is also a group under the same group operation as G; we write $H \leq G$.

Lemma 1.3.1 *If $H \leq G$, $e_H = e_G$ and $h_H^{-1} = h_G^{-1}$. Also, for $H \neq \emptyset$ and $H \subseteq G$, $H \leq G$ iff for all $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$.*

Proof Let e_h be the identity in H, and note that $e_H = e_H e_H$. Now, e_H will have inverse e_H^{-1} in G, so

$$e_G = e_H^{-1} e_H = e_H^{-1} e_H e_H = e_G e_H = e_H$$

as required. Similar,y suppose h has inverse h_G^{-1} in G and h_H^{-1} in H, then

$$h_G^{-1} = h_G^{-1} e = h_G^{-1}(h h_H^{-1}) = (h_G^{-1} h) h_H^{-1} = e h_H^{-1} = h_H^{-1}.$$

Since G is associative by assumption, and $H \subseteq G$, H inherits associativity. Since $H \neq \emptyset$, there exists $h \in H$. By previous part, $hh^{-1} = e \in H$, so the identity exists in H, and thus the inverse exists also in H. For $h, g \in H$, $g^{-1} \in H$, then $h(g^{-1})^{-1} = hg \in H$, so we have closure, and thus H is a group. ■

Example 1. Let $\mathbb{C}^*$ be the group of non-zero complex numbers under multiplication, and let

$$H = \{\mathrm{e}^{2\pi \mathrm{i} k/n} \mid 0 \leq k < n,\ n \geq 2\}.$$

Since $\mathrm{e}^{2\pi \mathrm{i} k_1/n}(\mathrm{e}^{2\pi \mathrm{i} k_2/n})^{-1} = \mathrm{e}^{2\pi \mathrm{i}(k_1-k_2)/n} \in H$ taking $k_1 - k_2$ in mod n, $H \leq \mathbb{C}^*$ by previous lemma. (In fact $H \cong \mathbb{Z}_n$).

2. For S_n the group of permutations, let A_n be the subset of all even permutations in S_n. (A_n is known as the **alternating group**.) To show $A_n \leq S_n$, we have that

$$\sigma = (a_1 b_1) \cdots (a_k b_k), \qquad \Rightarrow \qquad \sigma^{-1} = (a_k b_k) \cdots (a_1 b_1).$$

We see the parity of σ and σ^{-1} are equal, so for any two permutations $\sigma, \tau \in A_n$, $\sigma\tau^{-1}$ is an even permutation, and thus $A_n \leq S_n$. (Note also that $|A_n| = n!/2$.)

For all G, $\{e\}$ and G are also subgroups of G, known as the **improper subgroups** of G.

1.3.2 *Order and cosets*

The **order** of an element $g \in G$, denoted $|g|$, is the least positive integer n such that $g^n = e$ if $n < \infty$, otherwise they are of infinite order.

Proposition 1.3.2 *Let $g \in G$, with $|g| = n < \infty$. Then the set $\langle g \rangle]\{g^k \mid 0 \leq k < n\}$ is a subgroup of G, known as the **cyclic group** generated by g.*

Proof Let $t \in \mathbb{Z}^+$, then $t = qn + r, 0 \leq r < n$. So $g^t = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r$, so we have closure. Associativity follows since $\langle g \rangle \subseteq G$. Identity exists by definition, and $(g^k)^{-1} = g^{n-k}$ is the inverse. ∎

The order of a group is the number of elements of G, denoted $|G|$.

Theorem 1.3.3 *Any group of prime order is cyclic. Any non-identity element can be the generator of the group.*

To proof this, we make use of the following theorem:

Theorem 1.3.4 (Lagrange) *If $H \leq G$, then $|H|$ divides $|G|$.*

Proof of theorem above Let $g \in G$, and $g \neq e$. By Lagrange's theorem, $|\langle g \rangle|$ divides $|G| = p$, and since p is prime and $g \neq e$, $|\langle g \rangle| = p$, and $\langle g \rangle = G$. ∎

To proof Lagrange's theorem, we make use of the idea of **cosets**. For $H \leq G$ and $g \in G$, the **right coset of** H **in G** is the set $gH = \{gh \mid h \in H\}$, whilst the **left coset of** H **in G** is the set $Hg = \{hg \mid h \in H\}$.

Lemma 1.3.5 *We have the following:*

1. *Let X be a finite subset of a group G, and $g \in G$. Define gX and Xg like cosets, then $|gX| = |Xg| = |X|$.*
2. *If $gH \cap g'H \neq \emptyset$, then $gH = g'H$, and similarly for right cosets.*
3. *The union of all left cosets of G in G is the whole of G, and similarly for right cosets.*

Proof In order:

1. Let $x \neq x'$, $x, x' \in X$. If $gx = gx'$, then $g^{-1}gx = g^{-1}gx'$ which implies $x = x'$, and we have a contradiction, thus $x = x'$. the list is still unchanged in terms of size, so $|gX| = |X|$ and similarly for $|Xg|$.
2. Assuming $gH \cap g'H \neq \emptyset$. Let $x \in gH \cap g'H$, then there exists $h, h' \in H$ such that $x = gh = g'h'$, so

$$g = ge = (gh)h^{-1} = (g'h')h^{-1}.$$

Let $y \in gH$, $y = gh''$, then $(g'h'h^{-1})h'' = g'(h'h^{-1}h'')$, and since H is a group and is closed, $h'h^{-1}h'' \in H$, so $y \in g'H$, therefore $gH \subseteq g'H$. Similar arguments give $g'H \subseteq gH$, so $gH = g'H$.

3. Let $g \in G$, then $g = ge = eg$, and since $e \in H$, $g \in gH$ and $g \in Hg$ for all $g \in G$, so the union of all cosets covers all of G. ■

In summary:

- the size of a coset is the same as the set it is being acted on;
- all left cosets are either equal or disjoint, and similarly with right cosets;
- the union of all cosets is the group;
- left coset is equal to right coset if the group being acted on is abelian.

Proof of Lagrange's theorem $|G|$ is equal to the number of cosets that are distinct, multiplied by the size of the cosets (which is common to all cosets). Now, $H = eH$, so the common coset size is $|H|$, and $|H|$ divides $|G|$ as required. ■

Note that it didn't matter whether we used right or left cosets, so the number of right cosets is equal to the number of left cosets.

Corollary 1.3.6 *If $g \in G$, then $|g|$ divides $|G|$.*

Proof Let $H = \langle g \rangle$, then $|g| = |\langle g \rangle|$. Since $|H|$ divides $|G|$, $|g|$ divides $|G|$. ■

The **index** $|G : H|$ is the number of left (right) cosets of H in G that are distinct. So Lagrange's theorem may be restated as

$$|G| = |G : H| \cdot |H|.$$

Example We note that $A_n \leq S_n$. Consider the transposition $(12) \notin A_n$. Let σ be an odd permutation, so that $(12)\sigma \in A_n$. Then observe that $(12)(12)\sigma = e\sigma = \sigma \in (12)A_n$, so all odd permutations are in the coset $(12)A_n$.

A permutation is either even or odd, hence

$$S_n = A_n \cup (12)A_n, \qquad |S_n : A_n| = 2 \qquad \Rightarrow \qquad |A_n| = n!/2$$

because $|S_n| = n!$. This also shows that there are as many even permutations in S_n as odd permutations.

1.3.3 *Isomorphisms*

A group G is isomorphic to H if there exists $\phi : G \to H$ where ϕ is a:

1. **homomorphism** – For all $g_1, g_2 \in G$, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$;

2. **epimorphism** (surjectivity) – For all $h \in H$, there exists $g \in G$ such that $\phi(g) = h$;

3. **monomophism** (injectivity) – For all $g_1, g_2 \in G$, $\phi(g_1) = \phi(g_2)$ implies that $g_1 = g_2$.

The first property says that the group structure is perserved, and the other two says that ϕ is a bijection.

Lemma 1.3.7 *$\phi : G \to H$ is a homomorphism iff:*

1. *For all $\phi(g) = e_H$, $g = e_G$;*

2. *for all $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$.*

Proof Let $h = \phi(e_G)$, then

1. $hh = \phi(e_G)\phi(e_G) = \phi(e_G e_G) = \phi(e_G) = h$, so $h = e_H$.

2. $e_h = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$, so $\phi(g^{-1}) = (\phi(g))^{-1}$.

■

Example Examples of homomorphisms include

$$\phi : S_3 \to \{\pm 1\}, \qquad \phi(\sigma) = \begin{cases} +1, & \text{if } \sigma \text{ even,} \\ -1, & \text{if } \sigma \text{ odd,} \end{cases}$$

$$\phi : \mathbb{Z} \to \mathbb{Z}, \qquad \phi(n) = kn,$$

$$\phi : \mathbb{Z}_3 \to A_3, \qquad \phi(\bar{0}) = e, \qquad \phi(\bar{1}) = (123), \qquad \phi(\bar{2}) = (132).$$

1.4 *Symmetry*

A **symmetry** on an object is a function that sends the object to itself and preserves the basic structure of the object. For example, for an equilateral triangle with vertices labelled $1, 2, 3$, we have In fact,

Symmetry	permutation
Reflection, $1, 2, 3$ invariant	$(23), (13), (12)$
Rotation, $(2\pi/3)^n$ anti-clockwise, $n = 0, 1, 2$	$e, (132), (123)$

this group it complete as there are no more ways to permute the numbers. This forms the **dihedral group** D_3.

Now consider the square, and we have symmetries We see that $\{e, r, r^2, r^3\}$ form a cyclic group with r as the generator, which appears to be a subgroup of order four in D_4. Another thing to notice is that all reflections are inverses of themselves, so that $\{e, v\}$, $\{e, h\}$,

Symmetry	symbol
Rotation, $(\pi/2)^n$ anti-clockwise, $n = 0, 1, 2, 3$	e, r, r^2, r^3
Vertical reflection	v
Horizontal reflection	h
Leading diagonal reflection	d_1
Off-diagonal reflection	d_2

$\{e, d_1\}$, $\{e, d_2\}$ are also subgroups of D_4. Further, it may be shown that

$$rh = d_1, \qquad r^2h = v, \qquad r^3h = d_2,$$

so it seems that we can generate D_4 using r and h (or indeed any of the reflections together with a rotation).

For a regular n-gon, we let r be the rotation by $2\pi/n$, and h to be any reflection. These then have the relations

$$r^n = e, \qquad h^2 = e, \qquad (rh)^2 = e, \qquad rh = hr^{-1},$$

and $D_n = \{e, r, \cdots r^{n-1}, h, rh \cdots r^{n-1}h\}$ forms a group of order $2n$. (Note that for a regular n-gon, there are $2n$ lines of reflection although only n of them are distinct.) Further, rotational symmetries form a cyclic group of order n, generated by r, which is a subgroup of D_n with index two, whilst reflectional symmetries form a subgroup of order two, generated by each individual reflection, of index n.

Example Find all the subgroups of order four in D_8.

The subgroup either has an element of order four, or has identity and three order two elements.

1. Since $|r^2| = 4$, $\{e, r^2, r^4, r^6\} \leq D_8$.

2. All reflections and r^4 have order four. A subgroup of this type must contain at least two reflections, r^ih and r^jh say, with $(i > j)$. Now,

$$r^ihr^jh = r^ir^{-j}hh = r^{i-j} \neq e,$$

so it is a rotation thus r^4, which implies that $i = 4 + j$. Hence the subgroups of this type are

$$\{e, r^4, h, r^4h\}, \qquad \{e, r^4, rh, r^5h\}, \qquad \{e, r^4, r^2h, r^6h\}, \qquad \{e, r^4, r^3h, r^7h\}.$$