MA2202

Algebra I

Jia Xiaodong

December 3, 2020

1 Integers

In this section we briefly restate some number theory theorems and proofs. It is assumed that most of these have been seen before and so we will try to be brief.

Theorem 1.1 (Division algorithm)**.** *Let $x, y \in \mathbb{Z}$ with $y \neq 0$. There exists unique integers q and r such that*

$$x = qy + r \qquad 0 \leq r < |y|$$

r is also called the remainder *of x divided by y.*

Proof. First we show existence. Consider

$$\dots, x + 3|y|, x + 2|y|, x + |y|, x - 3|y|, x - 2|y|, \dots$$

which is a string of decreasing integers. Thus there exists $t \in \mathbb{Z}$ such that

$$x - t|y| \geq 0 > x - (t+1)|y|$$

Set $r = x - t|y|$ and so

$$r \geq 0 > r - |y|.$$

Then by choosing either $q = -t$ or $q = t$, we can get

$$x = r + qy.$$

Next we prove uniqueness. Suppose

$$x = qy + r = q'y = r'$$

Then

$$r - r' = y(q' - q)$$

Since $0 \leq r, r' < |y|$, we get $|y| > |r' - r| = |y||q' - q|$. For y cannot be greater than a positive multiple of itself, so $|q' - q| = 0$. Thus we get $q = q'$ and $r = r'$. ■

Lemma 1.2. *Let $x, y \in \mathbb{Z}$ and $y \neq 0$. Let $x = qy + r$ where $0 \leq r \leq |y|$. Then*

$$\gcd(x, y) = \gcd(y, r).$$

Proof. An integer c divides x and y iff it divides y and r. The set of common divisors of x and y is the same as the set of common divisors of y and r, hence their gcd is also the same. ■

This gives us an effective way of computing the $\gcd(x_1, x_2)$, also known as the Euclidean algorithm.

- If $x_2 < 0$ then $\gcd(x_1, x_2) = \gcd(x_1, |x_2|)$.
- If $x_2 = 0$ then $\gcd(x, x_2) = |x|$.
- Otherwise, using the division algorithm write $x_1 = qx_2 + x_3$ where $0 \leq r < y$. Then $\gcd(x_1, x_2) = \gcd(x_2, x_3)$.

$$\gcd(x_1, x_2) = \gcd(x_2, x_3) = \dots$$

where $x_2 > x_3 > \dots \geq 0$. The division algorithm prevents $x_n < 0$, so the algorithm stops whenever $x_n = 0$.

Theorem 1.3 (Bézout's Identity). *Let $d = \gcd(x, y)$ where $y \neq 0$. Let*

$$I = \{mx + ny : m, n \in \mathbb{Z}\}$$

then $I = d\mathbb{Z}$ is the set of all multiples of d.

Proof.

($I \supseteq d\mathbb{Z}$): $d \in I$ because by observing the Euclidean algorithm we find that the remainder x_{n+2} is always a linear combination of x_n and x_{n+1}. Therefore d can be expressed as a linear combination of $x_1 = x$ and $x_2 = y$ alone, and so can any multiple of d.

($I \subseteq d\mathbb{Z}$): We can always write $x = x'd$ and $y = y'd$ so $mx + ny = d(mx' + ny')$ is a multiple of d. Thus all elements in I are multiples of d. ■

More specifically, this states that there exists a linear combination $mx + ny = d$ iff $d = \gcd(x, y)$.

Definition 1.1 (Modulo). We write $a \equiv b \pmod{m}$ if $m \mid (a - b)$. □

$\equiv$ forms an equivalence relation on $\mathbb{Z}$. Furthermore it can be shown that $a \equiv b \pmod{m}$ iff a and b have the same remainder when divided by m.

Theorem 1.4 (Fermat's Little Theorem). *Let p be a prime number. Then*

$$n^p \equiv n \pmod{p}.$$

Proof. The case is true for $n = 0$. Suppose the statement is true for some $n = k$. Consider the case when $n = k + 1$:

$$\begin{aligned}(k+1)^p - (k+1) &= \sum_{i=0}^{p} \binom{p}{i} k^i - (k+1) \\ &= \sum_{i=1}^{p-1} \binom{p}{i} k^i + k^p - k.\end{aligned}$$

By the inductive hypothesis $p \mid k^p - k$. Furthermore, for any i such that $0 < i < p$,

$$p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\dots(p-i+1)}{i!}.$$

Then looking back at the summation, we are done. Hence by induction the claim is true for all n. ■

Corollary 1.4.1. *If a prime integer p does not divide n then $n^{p-1} \equiv 1 \pmod p$.*

Proof. p divides $n^p - n = n(n^{p-1} - 1)$. If it does not divide n then it has to divide $n^{p-1} - 1$. ■

Theorem 1.5 (Chinese Remainder Theorem)**.** *Suppose* $\gcd(m, n) = 1$*. Then the equations*

$$\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod n \end{aligned}$$

has a common solution $x \pmod{mn}$.

Proof. Since $\gcd(m, n) = 1$, there exist some $s, t \in \mathbb{Z}$ such that $sm + tn = 1$. Therefore

$$\begin{aligned} tn &\equiv 1 \pmod m \\ sm &\equiv 1 \pmod n \end{aligned}$$

Then $x = atn + bsm$ is a solution.

Suppose there is another solution x'. Then both m and n divides $x - x'$. Thus mn also divides $x - x'$. Therefore

$$x \equiv x' \pmod{mn}$$

■

Theorem 1.6 (Fundamental theorem of arithmetic)**.** *Given $n \in \mathbb{Z}$ and $n > 1$, there exists a unique factorization*

$$n = p_1 p_2 \dots p_n$$

where p_i's are primes.

Proof. Perform strong induction on n. For $n = 2$ this is trivial. Suppose the claim holds for all positive integers smaller than some $n = k$. If n is prime then we are done. Otherwise we can write $n = ab$ where $a, b > 1$. By the inductive hypothesis a and b both have a prime decomposition and therefore so does n. This is also unique. Supposing the contrary, i.e. there are two different decompositions

$$n = p_1 \dots p_j = q_1 \dots q_k$$

where p_i and q_i are primes. Now p_1 divides $q_1 \dots q_k$ and hence also one of the q_i's, let that be q_1. However since q_1 is prime this means $p_1 = q_1$ and $p_2 \dots p_j = q_1 \dots q_k < n$. This contradicts the inductive hypothesis. ■

Theorem 1.7. *Suppose*

$$x = \prod_i p_i^{e_i}, \qquad y = \prod_i p_i^{f_i}, \qquad d = \prod_i p_i^{g_i}$$

are prime factorizations of integers x, y, d, where all p_i's are distinct primes and $e_i, f_i, g_i \geq 0$ for all i. Then

i. $d \mid x \iff g_i \leq e_i$ *for all i.*

ii. $d \mid x \wedge d \mid y \implies g_i \leq \min(e_i, f_i)$ *for all i.*

iii. $\gcd(x, y) = \prod_i p_i^{\min(e_i, f_i)}$.

iv. $d \mid x \wedge d \mid y \implies d \mid \gcd(x, y)$.

Proof.

i. $d \mid x \iff x = ad$ for some $a \in \mathbb{Z}$. By the fundamental theorem of arithmetic there exist some prime factorization for a as well. If we let $a = \prod_i p_i^{h_i}$ then

$$x = \prod_i p_i^{e_i} = \prod_i p_i^{h_i + g_i}$$

which makes it quite evident that $g_i \leq e_i$ since the factorization has to be unique.

ii. From (i), $g_i \leq e_i$ and $g_i \leq f_i$ for all i, i.e. $g_i \leq \min(e_i, f_i)$.

iii. Let $b = \gcd(x, y)$, and let $b = \prod_i p_i^{k_i}$. By (ii), $k_i \leq \min(e_1, f_i)$. However, to be the largest, all exponents have to be exactly $\min(e_i, f_i)$.

iv. This is evident from (ii) and (iii).

■

Theorem 1.8. *Take any two non-zero integers m and n that are coprime, i.e.* $\gcd(m, n) = 1$.

i. There is no common prime divisor in the prime factorization of m and n.

ii. If $m \mid x$ and $n \mid x$ then $mn \mid x$.

Proof.

i. Suppose there were some such common prime divisor p. Then $p \geq \gcd(m, n)$, a contradiction.

ii. We can see this from (i), and Theorem 1.7 (i).

■

2 Introduction to groups

2.1 Binary operations

Definition 2.1. Let G be a set. A *binary operation* $*$ on G is a function

$$* : G \times G \to G.$$

We frequently denote $*(x, y)$ as $x * y$. □

Definition 2.2. Let $*$ be a binary operation on a set G.

- It is called *associative* if

$$\forall a, b, c \in G \ [(a * b) * c = a * (b * c)]$$

- It is called *commutative* or *abelian* if

$$\forall a, b \in G \ [a * b = b * a]$$

□

Definition 2.3. Let $(G, *)$ be a set with a binary operation. Let $e \in G$.

- e is called a *left identity element* if $\forall a \in G \ (e * a = a)$.
- e is called a *right identity element* if $\forall a \in G \ (a * e = a)$.
- e is called an *identity element* iff it is both a left and right identity element.

□

The identity element is unique since if e' is another identity then $e' = e * e' = e$. In some places it is also represented by 1.

2.2 Group Axioms

There are many equivalent definitions of a group, but the following four axioms are universally accepted.

Definition 2.4 (Group Axioms)**.** A group $(G, *)$ consists of a set G and a binary operation $*$ on G which satisfy the following axioms:

G1. Closure: $\forall a, b \in G \ (a * b \in G)$.

G2. Associativity: $\forall a, b, c \in G \ [(a * b) * c = a * (b * c)]$.

G3. Existence of identity: $\exists e \in G, \forall a \in G \ [e * a = a * e = a]$.

G4. Existence of inverse: $\forall a \in G, \exists b \in G \ [a * b = b * a = e]$.

□

We may omit the symbol for the group operation in the future, i.e. we write ab instead of $a * b$.

The inverse of any group element is unique. If b, b' are both inverses of a then $b = b(ab') = (ba)b' = b'$. Hence we can safely denote it by a^{-1}. The identity element is also unique, since if $e'a = a = ea$ it is clear that $e' = e$. So we will usually denote the identity element as e.

Definition 2.5. For any element x of a group, we write

$$\underbrace{x * \cdots * x}_{n \text{ times}} = x^n$$

□

Theorem 2.1. *The following are true:*

- $(a^{-1})^{-1} = a$.
- $(a * b)^{-1} = b^{-1} * a^{-1}$.
- $a^{-1} * \cdots * a^{-1} = (a * \cdots * a)^{-1}$ *where there are* n *copies on both sides. We can call this* a^{-n}.
- $a * c = b * c \implies a = b$.
- *For any* $a, b \in G$, *the equation* $a * x = b$ *has an unique solution* $x \in G$.
- *If* $m, n \in \mathbb{Z}$, *then* $a^n * a^m = a^{n+m}$.

Proof. TODO ■

Theorem 2.2. *If* $(G, *)$ *is a group in which* $x^2 = e$ *for all* $x \in G$, *then it is abelian.*

Proof.

$$\begin{aligned} ab * ab &= e \\ (abab)ba &= ba \\ aba(bb)a &= ba \\ ab &= ba \end{aligned}$$

■

Example 2.1. The *general linear group* of rank n, written $\mathbf{GL}(n, \mathbb{F})$ is the set of $n \times n$ invertible matrices over some field $\mathbb{F}$. The group operation is the usual matrix multiplication.

The identity element is the identity matrix $\mathbf{I}_n$ and the usual inverse matrix of a is a^{-1}. Of course $\mathbf{GL}(n, \mathbb{F})$ is not abelian for $n \geq 2$ as we known matrix multiplication is not commutative in general. ♢

Example 2.2. The *special linear group* of rank n, written $\mathbf{SL}(n, \mathbb{F})$ is the set of $n \times n$ matrices with determinant 1 over some field $\mathbb{F}$. The group operation is the usual matrix multiplication.

The identity element is the identity matrix $\mathbf{I}_n$ and the usual inverse matrix of a is a^{-1}. It is contained within $\mathbf{GL}(n, \mathbb{F})$. ♢

Theorem 2.3. *Let there be a set G and a binary operation $*$ on G satisfying the following weaker axioms:*

G1. Closure.

G2. Associativity.

RG3. Existence of right identity: $\exists e \in G, \forall a \in G\ (a * e = a)$.

RG4. Existence of right inverse: $\forall a \in G, \exists b \in G\ (a * b = e)$.

Then $(G, *)$ is a group.

Proof. A group would satisfy all of them. So what we have to do is to check the other direction. ■

The proposition will also still be valid if we changed the right identity and inverse into the left identity and inverse.

2.3 Examples of groups

Example 2.3. A group cannot be an empty set since the identity element has to always exist. A group with a single identity element is called the *trivial* group. ◊

Example 2.4. Standard examples of abelian groups are $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, equipped with the usual operation of addition $+$. The (additive) identity element is 0 and the (additive) inverse is $-x$. ◊

Example 2.5. A vector space over a field with vector addition $+$ forms a group. The identity element is the zero vector, and the inverse element of vector $\mathbf{v}$ is $-\mathbf{v}$. ◊

Example 2.6. Given a positive integer n, and let

$$\mu_n = \{\exp\left(\frac{2k\pi i}{n}\right) : k = 0, \ldots, n-1\}$$

which are the n roots of unity in $\mathbb{C}$. $(\mu_n, \times)$ forms a finite abelian group of order n with the usual complex multiplication operation $\times$. This is called the *cyclic group* of order n. ◊

Example 2.7. Together with addition modulo n, the set

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

also forms a group. This odd notation will be explained in the future. This is also called the cyclic group of order n. The reason for this name will become clear later on. ◊

Example 2.8. Let Y be a set (potentially infinite), and let

$$S_Y = \{f : Y \to Y \mid f \text{ is a bijection}\}.$$

Then $(S_Y, \circ)$ is a group. The identity element is the identity function, and the inverse element is is its inverse function.

Furthermore, if $Y = \{1, \ldots, n\}$, then S_Y is a finite group of order $n!$. We call this the *symmetric group* on n letters, denoted by $(S_n, *)$. ◊

Example 2.9. Let $(G, *)$ and $(H, \star)$ be two groups. Define a new binary operation $\cdot$ on $G \times H$ by

$$(g, h) \cdot (g', h') = (g * g', h \star h').$$

Then $(G \times H, \cdot)$ forms a group called the *product group* of $(G, *)$ and $(H, \star)$. The identity element is (e_G, e_H) where e_G is the identity of G and e_H is the identity of H. The inverse element of (g, h) is (g^{-1}, h^{-1}). $\diamondsuit$

Example 2.10. Consider

$$\mathbb{H} = \left\{ \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix} \mod z_1, z_2 \in \mathbb{C} \right\}.$$

Let $\mathbb{H}^\times$ denote the subset of non-zero matrices in $\mathbb{H}$. Then $(\mathbb{H}^\times, \times)$ forms a group, with ordinary matrix multiplication $\times$. This is known by names like Hamiltonian algebra, skew-field, etc. Indeed, $(H, +, \times)$ is almost a field, except that $(\mathbb{H}^\times, \times)$ is non-abelian. $\diamondsuit$

3 Group isomorphisms

In our examples we gave different groups the same names. The reason for this is that they behave in the same way. If we were to write the multiplication table for μ_n and $\mathbb{Z}/n\mathbb{Z}$ we would find that they look very similar. We call these groups isomorphic.

Definition 3.1. Let $(G, *)$ and $(H, \star)$ be two groups. We say that they are *isomorphic* if there exists a bijection $\phi : G \to H$ such that

$$\forall g_1, g_2 \in G \; [\phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2)]$$

Furthermore ϕ is called a *group isomorphism* and we write $(G, *) \cong (H, \star)$. $\square$

Isomorphisms are a more restricted case of homomorphisms.

Definition 3.2. Let $(G, *)$ and $(H, \star)$ be two groups. If there is a function $\phi : G \to H$ such that

$$\forall g_1, g_2 \in G \; [\phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2)]$$

we say ϕ is a *group homomorphism.* $\square$

Example 3.1. $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ with group isomorphism

$$\phi(m) = \exp\left(\frac{2k\pi i}{m}\right).$$

Using the property of the exponential function we can see that this is indeed true. $\diamondsuit$

Example 3.2. $\mu_n \cong (G, *)$ where

$$G = \{e = a^n, a, a^2, \dots, a^{n-1}\}$$

Again this is easily seen to be true. We call any group that can be written in the form of G a *cyclic group of order n.* $\diamondsuit$

Theorem 3.1. *If $(G, *)$ and $(H, \star)$ are two groups and $\phi : G \to H$ is a homomorphism, and e_G and e_H are the identity elements of G and H respectively, then* *i.* $\phi(e_G) = e_H$.

ii. $\forall g \in G \left[\phi(g^{-1}) = (\phi(g))^{-1}\right]$.

Proof.

i.

$$\begin{aligned} \phi(e_G) &= \phi(e_G * e_G) \\ &= \phi(e_G) \star \phi(e_G) \\ e_H \star \phi(e_G) &= \phi(e_G) \star \phi(e_G) \end{aligned}$$

Cancellation (see theorem 2.1) then tells us that $e_H = \phi(e_G)$.

ii.

$$\begin{aligned} \phi(g)\phi(g^{-1}) &= \phi(gg^{-1}) \\ &= \phi(e_G) \\ &= e_H \end{aligned}$$

■

Theorem 3.2. *Suppose $\phi : G \to H$ and $\psi : H \to K$ are two isomorphisms. Then*

i. $\phi^{-1} : H \to G$.

ii. $\psi \circ \phi : G \to K$.

are also group isomorphisms.

Proof.

i. Since ϕ is bijective then ϕ^{-1} is also bijective. For any $g, h \in H$, $\phi^{-1}(g), \phi^{-1}(h) \in G$.

$$\begin{aligned} \phi(\phi^{-1}(g)\phi^{-1}(h)) &= \phi(\phi^{-1}(g))\phi(\phi^{-1}(h)) \\ &= gh \end{aligned}$$

Therefore

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

ii. Compositions of bijections yield a bijection. For any $g, h \in G$,

$$\begin{aligned} \psi\phi(gh) &= \psi(\phi(g)\phi(h) \\ &= \psi(\phi(g))\psi(\phi(h)). \end{aligned}$$

■

Theorem 3.3. *Suppose $(G, *)$ and $(H, \star)$ are isomorphic non-abelian groups. There are at least two distinct isomorphisms.*

Proof. TODO ■

4 Subgroups

Definition 4.1. Let $(G,*)$ be a group. Let $H \subseteq G$. Then if $(H,*)$ forms a group, we call it a *subgroup* of G. □

G and the identity $\{e\}$ are subgroups as well. They are called the trivial subgroups.

Lemma 4.1. *$(d\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$.*

Theorem 4.2. *Suppose $(I,+)$ is a subgroup of $(\mathbb{Z},+)$. Then $I = d\mathbb{Z}$ for some non-negative integer d.*

Proof. If $I = \{0\}$ then $d = 0$.

Otherwise it has a non-zero element x. Since I is a group, it also contains $-x$. Hence I contains at least one positive integer. Let d be the smallest positive integer in I.

$(I \supseteq d\mathbb{Z})$: $d + \cdots + d \in I$. The same goes for negative elements.

$(I \subseteq d\mathbb{Z})$: Take any $x \in I$. Using the division algorithm we can write $x = qd + r$ where $0 \leq r < d$. Since $qd \in I$, $r = x - qd \in I$. However d is the smallest positive integer in I, which means $r = 0$ and so $x = qd \in d\mathbb{Z}$. ■

Theorem 4.3. *All the subgroups of $(\mu_n,\times)$ are of the form $(\mu_m,\times)$ where $m \mid n$.*

Proof. For convenience let us write $e(d) = \exp\left(\frac{d(2\pi i)}{n}\right)$. Let $(H,\times)$ be a subgroup of $(\mu_n,\times)$. $H = \{1\}$ is the trivial case.

Otherwise it contains $e(d)$ for some $0 < d < n$. Let d be the smallest positive integer d such that $e(d) \in H$. Using the division algorithm we can write $n = md + r$ where $0 \leq r < d$. Then

$$\begin{aligned} 1 &= e(n) \\ &= e(md + r) \\ &= e(d)^m e(r) \\ e(r) &= e(d)^{-m} \in H \end{aligned}$$

But the way d is chosen means that $r = 0$ and therefore $n = md$.

$(H \supseteq \mu_m)$: Since H is a group $e(0), e(d), e(2d) \ldots e((m-1)d) \in H$.

$(H \subseteq \mu_m)$: Take any $e(k) \in H$. Then by the division algorithm we can write $k = qd + t$ where $0 \leq t < d$. With the same reasoning as above we can show that $t = 0$. ■

The following theorem tells us that we do not need to check all the group axioms to establish if a subset is a subgroup.

Theorem 4.4. *Let $(G,*)$ be a group and let $H \subseteq G$ be a non-empty subset. Then $(H,*)$ is a subgroup iff*

i. It is closed under $*$, and

ii. inverse elements exist.

Proof. This is fairly obvious since the properties of $*$ are inherited from G. ■

Theorem 4.5. *Let $(G,*)$ be a group and let $H \subseteq G$ be a non-empty subset. Then $(H,*)$ is a subgroup iff*

$$\forall a,b \in H \; [a * b^{-1} \in H]$$

Proof. By choosing $a = b$ we can guarantee the existence of inverse elements, and then using that we can show that H is closed under $*$. ■

Theorem 4.6. *Let $(G,*)$ be a group and let $H \subseteq G$ be a non-empty* finite *subset. Then $(H,*)$ is a subgroup iff*

$$\forall a,b \in H \; [a * b \in H]$$

Proof. All we need now is to find the inverse elements. The statement implies that $a^i \in H$ for all $i = 1, 2, \ldots$. Since H is finite, it must be that $a^n = a^m$ for some $n > m$. Then $a^{-1} = a^{n-m-1}$. ■

Theorem 4.7. *If $\{(H_i,*) \mid i \in I\}$ is a collection of subgroups of $(G,*)$, then $(\bigcap_{i\in I} H_i, *)$ is a subgroup of $(G,*)$.*

Proof. If $a, b \in \bigcap_{i\in I} H_i$, then a, b are elements of all H_i for all $i \in I$. Then $a * b^{-1} \in H_i$ as well, and so $a * b^{-1} \in \bigcap_{i\in I} H_i$. ■

Theorem 4.8. *Let $(H,*)$ and $(K,*)$ be subgroups of $(G,*)$. If $(H \cup K, *)$ is a subgroup, then either $H \subseteq K$ or $K \subseteq H$.*

Proof. Take $h \in H$ and $k \in K$. Since $H \cup K$ is a subgroup, this means that $h * k \in H \cup K$. Therefore either $h * k \in H$ or $h * k \in K$. Since H and K themselves are groups, this means that either $h * k * h^{-1} = k \in H$ or $h * k * k^{-1} = h \in K$. ■

Definition 4.2 (Generators)**.** Let G be a group and X be a subset of G. Then the smallest subgroup of G containing X is denoted $\langle X \rangle$ and called the subgroup *generated by* X. If X is finite then we say that $\langle X \rangle$ is *finitely generated.* □

Definition 4.3 (Words)**.** TODO □

5 Symmetric groups

5.1 Permutations

Definition 5.1 (Permutations)**.** A permutation of a set A is a bijective function $f : A \to A$. □

Example 5.1. Let $A = \{1, 2, 3\}$. Then f defined by $f(1) = 3$, $f(2) = 2$, and $f(3) = 1$, is a permutation of A. We can also write it in this way:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

◊

Definition 5.2 (Symmetric group)**.** Let $X = \{1, 2, \ldots, n\}$ and

$$S_n = \{f : X \to X \mid f \text{ is a bijection}\}.$$

Then $(S_n, \circ)$ is called the *symmetric group* or *permutation group* on n letters, where $\circ$ denotes composition. □

Its name is justified.

Theorem 5.1. $(S_n, \circ)$ *forms a group.*

Proof. We check the axioms.

G1. Take any $f, h \in S_n$. Composing bijections still form a bijection so $f \circ g \in S_n$.

G2. Composition is associative.

G3. The identity function $e(x) = x$ is the identity element. First of all $e(x)$ is bijective so it is in S_n. Furthermore we can check that $f \circ e = e \circ f = f$.

G4. A bijection f have a corresponding inverse function f^{-1} and $f \circ f^{-1} = e$.

■

In fact, what is in X is unimportant. X does not even have to be finite.

Definition 5.3 (Symmetric group)**.** Let X be an arbitrary set. We define

$$S_X = \{f : X \to X \mid f \text{ is a bijection}\}.$$

Then $(S_X, \circ)$ is also known as a symmetric group. □

It is justified to call it a group because we can reuse the same proof as above to show that it is indeed a group.

Theorem 5.2. *Let* $X = \{x_1, x_2, \ldots, x_n\}$ *be a set of* n *elements. Then* $(S_n, \circ) \cong (S_X, \circ)$.

Proof. Let $Y = \{1, 2, \ldots n\}$. Then we essentially want to find a bijection $\phi : S_n \to S_Y$.

Let $T : Y \to X$ be defined as $T(n) = x_n$ for $n \in Y$. This is obviously a bijection. For any $f \in S_n$. Define $\phi(f) = T \circ f \circ T^{-1}$. The composition of bijections form a bijection so ϕ is a bijection.

Now take $f, g \in S_n$.

$$\begin{aligned} \phi(f \circ g) &= T \circ f \circ g \circ T^{-1} \\ &= T \circ f \circ T^{-1} \circ T \circ g \circ T^{-1} \\ &= \phi(f) \circ \phi(g). \end{aligned}$$

■

5.2 Permutation matrices

Definition 5.4 (Permutation matrices)**.** A permutation matrix is a matrix where its columns are a permutation of the standard basis vectors. □

Example 5.2. Let S'_3 denote the set of all 3 by 3 permutation matrices, and × the regular matrix multiplication. Then $(S'_3, \times)$ forms a group.

◊

More generally,

Theorem 5.3. $(S'_n, \times)$*, the set of* n *by* n *permutation matrices equipped with standard matrix multiplication forms a group.*

Proof. We check the axioms one by one.

G1. A permutation matrix as a linear transformation is simply a bijection $B \to B$ where B is the standard basis. Hence multiplication acts as composition on these transformations, and thus S_n is closed under multiplication.

G2. Multiplication is associative.

G3. The identity matrix is in S_n and is the identity element.

G4. Since they are bijections each permutation matrix has an inverse.

■

Theorem 5.4. $(S'_n, \times) \cong (S_n, \circ)$.

Proof. We can define a group isomorphism $\phi : S_n \to S'_n$. Take $f \in S_n$, then define $T = \phi(f)$ be the linear transformation such that $T(\mathbf{e}_u) = \mathbf{e}_{f(i)}$. In other words

$$\phi(f) = \begin{pmatrix} \mathbf{e}_{f(1)} & \mathbf{e}_{f(2)} & \cdots & \mathbf{e}_{f(n)} \end{pmatrix}.$$

First we check that ϕ is a bijection. It is injective, because if $\phi(f) = \phi(g)$ then looking at the above it must be that $f(1) = g(1)$, $f(2) = g(2)$ and so on, so $f = g$. It is surjective since for every $T \in S'_n$ made up of some permutation of the basis vectors $\{\mathbf{e}_{i_1}, \dots .\mathbf{e}_{i_n}\}$ we can always find a $f \in S_n$ such that $f(j) = i_j$.

Now we have to show that is is an isomorphism. It is enough to show that for all standard basis vectors $\mathbf{e}_j$,

$$\phi(f \circ g) \times \mathbf{e}_j = (\phi(f) \times \phi(g)) \times \mathbf{e}_j$$

as linear transformations are defined by their action on the basis vectors. Multiplication with a standard basis column vector $\mathbf{e}_j$ effectively selects the j-th column.

$$\begin{aligned} \phi(f \circ g) \times \mathbf{e}_j &= \mathbf{e}_{(f \circ g)(j)} \\ &= \phi(f) \times \mathbf{e}_{g(j)} \\ &= \phi(f) \times \phi(g) \times \mathbf{e}_j. \end{aligned}$$

■

5.3 Cayley's theorem

Lemma 5.5. *Let G, G' be groups and let $\phi : G \to G'$ be an injective homomorphism. Then $\phi[G]$ is a subgroup of G' and ϕ is an isomorphism between G and $\phi[G]$.*

Proof. First we check that $\phi[G]$ forms a subgroup. We check the requirements of theorem 4.4.

Take $x', y' \in \phi[G]$. Then there exist respective pre-images $x, y \in G$. Then

$$\begin{aligned} x'(y')^{-1} &= \phi(x)(\phi(y))^{-1} \\ &= \phi(x)\phi(y^{-1}) \\ &= \phi(xy^{-1}) \in \phi[G] \end{aligned}$$

By theorem 4.5 $\phi[G]$ is a subgroup.

ϕ is surjective onto its own image, $\phi[G]$. Therefore it is an isomorphism. ■

Theorem 5.6 (Cayley's theorem)**.** *Every group is isomorphic to a permutation group.*

Proof. Let $(G, *)$ be a group. We will show that G is isomorphic to a subgroup of S_G.

For every $g \in G$, define $f_g : G \to G$ as $f_g(x) = gx$. Every f_g is injective. If $f_g(x) = gx = gy = f_g(y)$ then it is clear that $x = y$ by cancellation.

Now define $\phi : G \to S_G$ as $\phi(x) = f_x$. ϕ is injective. Suppose $\phi(x) = f_x = f_y = \phi(y)$. Then $f_x(e) = f_y(e)$ implies that $x = y$. ϕ is also a homomorphism, because for any $g \in G$,

$$\begin{aligned} f_{xy}(g) &= xyg \\ &= xf_y(g) \\ &= (f_x \circ f_y)(g). \end{aligned}$$

Recall that the group operation on S_G is composition $\circ$. Hence this shows that $\phi(xy) = \phi(x)\phi(y)$.

By lemma 5.5, ϕ provides an isomorphism between G and a subgroup of S_G. ■

5.4 Cycles and orbits

For some permutation σ, let us consider the relation $\sim$ defined as $a \sim b \iff b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. $\sim$ is in fact an equivalence relation. We quickly check this. Clearly $a = \sigma^0(a)$ so $a \sim a$. Furthermore if $a \sim b$ then $b = \sigma^n(a)$, but then $a = \sigma^{-n}(b)$ so $b \sim a$. If $a \sim b$ and $b \sim c$, then $b = \sigma^n(a)$ and $c = \sigma^m(b) = \sigma^{m+n}(a)$ so $a \sim c$.

Definition 5.5 (Orbits)**.** Let σ be a permutation of a set A. The equivalence classes in A by $\sim$ are called the *orbits* of A. □

Example 5.3. The orbits of the identity permutation are all single-element subsets. ◊

Example 5.4. The orbits of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 1 & 2 & 3 \end{pmatrix}$$

are $\{1,2,4,5\}$ and $\{3,6\}$. Under repeated action of σ, we obtain this pattern $1 \mapsto 5 \mapsto 2 \mapsto 4 \mapsto 1 \ldots$. We can also define another permutation μ that produces the same pattern:

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 1 & 2 & 6 \end{pmatrix}$$

the difference being we keep the other elements not involved fixed. ◊

This brings us to the idea of cycles.

Definition 5.6 (Cycles)**.** A permutation σ is a *cycle* if it has at most one orbit containing more than one element. The length of a cycle is the number of elements in its largest orbit. □

Theorem 5.7. *Two disjoint cycles in S_n commute.*

Proof. Let $c, c' \in S_n$ be two disjoint cycles. Express $c = (i_i, i_2, \ldots, i_s)$ and $c' = (j_1, j_2, \ldots, j_t)$. Take any $x \in \{1, 2, \ldots, n\}$. There are three cases to consider.

First if $x \in \{i_1, \ldots, i_s\}$, then $x \notin \{j_1, \ldots, j_t\}$. So we can write $x = i_k$ and $c(x) = i_{k+1}$ (addition is modulo s here). Therefore $(c \circ c')(x) = c(x) = c'(c(x)) = (c' \circ c)(x)$. The case where if $x \notin \{i_1, \ldots, i_s\}$, but $x \in \{j_1, \ldots, j_t\}$ is the same.

The last case is where $x \notin \{i_1, \ldots, i_s\}$, and $x \notin \{j_1, \ldots, j_t\}$. Then it is obvious that $(c \circ c')(x) = (c' \circ c)(x)$ in this case. ■

Theorem 5.8. *Let $c = (i_1, i_2, \ldots, i_n)$ be a cycle and $f \in S_n$. Then $f \circ c \circ f^{-1} = (f(i_1), f(i_2), \ldots, f(i_r))$.*

Proof. Take any $x \in \{1, \ldots, n\}$. Then there exists some y such that $x = f(y)$. Now if $y \in \{i_1, \ldots, i_r\}$, say $y = i_k$, then

$$(f \circ c \circ f^{-1})(x) = (f \circ c)(i_k) = f(i_k + 1).$$

Otherwise, if $y \notin \{i_1, \ldots, i_r\}$ this means that $f(y) \notin \{f(i_1), \ldots, f(i_r)\}$ so

$$(f \circ c \circ f^{-1})(x) = (f \circ c)(y) = f(y) = x.$$

■

Theorem 5.9. *Let $c = (i_1, i_2, \ldots, i_r) \in S_n$ be a cycle. Then $c' = (i_r, i_{r-1}, \ldots, i_1)$ is the inverse of c.*

Proof. This is easy to check, skipped. ■

Definition 5.7 (Transpositions)**.** A cycle of length 2 is a *transposition.* □

A more compact notation for writing cycles is the *cyclic notation.* In cyclic notation we write the cycle in a single row. For example, μ in the previous example becomes

$$\mu = (1, 5, 2, 4)$$

which expresses the fact that repeated applications of μ produces the pattern $1 \mapsto 5 \mapsto 2 \mapsto 4 \mapsto 1$, and that any other integer is left fixed.

Since cycles are permutations which are just functions, they can be composed. However there is no guarantee that the composition of two cycles give another cycle. For example σ from the examples above

$$\sigma = (1, 2, 4, 5)(3, 6).$$

In fact we can do this with any permutation.

Theorem 5.10. *Every permutation σ of a finite set is a product of disjoint cycles.*

Proof. Let $\mathcal{O}_1, \mathcal{O}_2, \ldots \mathcal{O}_n$ be the orbits of σ. Note that since orbits are equivalence classes they are disjoint sets. Let μ_i be the cycle defined by

$$\mu_i(x) = \begin{cases} \sigma(x), & \text{if } x \in \mathcal{O}_i \\ x & \text{otherwise} \end{cases}.$$

All μ_i are disjoint, since the orbits are disjoint in the first place. Then $\sigma = \mu_1 \mu_2 \cdots \mu_n$. ■

Corollary 5.10.1. *Every permutation σ of a finite set of at least 2 elements is a product of transpositions.*

Proof. This follows from the previous theorem and the fact that any cycle can be expressed as a product of transpositions:

$$(a_1, a_2, \ldots, a_n) = (a_1, a_n) \cdots (a_1, a_3)(a_1, a_2)$$

The checking of this part is skipped. ■

Theorem 5.11. *Consider the set of transpositions $C_n = \{(1, 2), (2, 3), \ldots, (n-1, n)\}$. The subgroup generated by C_n is S_n.*

Proof. Let the subgroup generated by C_n be called H_n. We perform induction on n. The statement is true for $n = 2$ since S_2 only has two elements, $e = (1, 2)(1, 2)$ and $(1, 2)$ itself.

Suppose the statement is true for some n. Now we consider the subgroup generated by C_{n+1}.

TODO ■

Corollary 5.11.1. *The transposition $\tau = (1, 2)$ and the cycle $\sigma = (1, 2, \ldots, n)$ generates S_n.*

Proof. First we note that

$$\begin{aligned}
\sigma(i, i+1)\sigma^{-1} &= \sigma(i, i+1) \begin{pmatrix} 1 & 2 & \cdots & i+1 & i+2 & \cdots & n-1 & n \\ n & 1 & \cdots & i & i+1 & \cdots & n-2 & n-1 \end{pmatrix} \\
&= \sigma \begin{pmatrix} 1 & 2 & \cdots & i+1 & i+2 & \cdots & n-1 & n \\ n & 1 & \cdots & i+1 & i & \cdots & n-2 & n-1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & \cdots & i+1 & i+2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & i+2 & i+1 & \cdots & n-1 & n \end{pmatrix} \\
&= (i+1, i+2)
\end{aligned}$$

where addition here is modulo n.

Therefore, we can see that

$$\sigma^i \tau \sigma^{-i} = (i+1, i+2)$$

■

5.5 The sign character

The sign character is used in calculating the determinant of matrices. Since $S_n' \cong S_n$, we can define it for permutations as well. We start with a polynomial

$$P(x_1, x_2, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

For example if $n = 3$ then

$$P(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

For any $f \in S_n$, form a new polynomial

$$P_f(x_1, x_2, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_{f(i)} - x_{f(j)}).$$

Since we only permute elements around and do not change their value, we make the observation that $P_f(\mathbf{x}) = \pm P(\mathbf{x})$.

Definition 5.8 (Sign character)**.** For $f \in S_n$, the sign character of f, written as $\operatorname{sgn}(f) = \pm 1$ is defined as

$$P_f(\mathbf{x}) = \operatorname{sgn}(f) P(\mathbf{x}).$$

If $\operatorname{sgn} f = 1$ we say f is an *even* permutation and otherwise we say that it is an *odd* permutation.

□

Theorem 5.12. *Let $f, g \in S_n$.*

i. $\operatorname{sgn}(f \circ h) = \operatorname{sgn}(f) \operatorname{sgn}(h)$.

ii. If f and h are both even (odd), then $f \circ h$ is also even (odd) respectively.

iii. If f is odd and h is even, then $f \circ h$ is odd.

iv. A transposition is an odd permutation.

v. A product of an even (odd) number of transpositions is an even (odd) permutation respectively.

Proof.

i.

$$\begin{aligned} P_{f \circ h}(\mathbf{x}) &= \prod (x_{f(h(i))} - x_{f(h(j))}) \\ &= P_f(x_{h(1)}, x_{h(2)}, \ldots, x_{h(n)}) \\ &= \operatorname{sgn}(f) P_h(\mathbf{x}) \\ &= \operatorname{sgn}(f) \operatorname{sgn}(h) P(\mathbf{x}). \end{aligned}$$

ii. Follows immediately from (i).

iii. Follows immediately from (i).

iv. For a transposition (i, j), exactly one of the terms in the product of the polynomial is flipped, namely the one containing x_i and x_j.

v. Follows immediately from (i) and (iii).

■

6 Cyclic groups

Definition 6.1. Let $(G, *)$ be a group and let $x \in G$. We call $\langle x \rangle = \{x^n \in G \mid n \in \mathbb{Z}\}$ the *cyclic subgroup* of G generated by x.

Furthermore, we define the order of $x \in G$ as $|\langle x \rangle|$. □

This definition is compatible with our notion of a generator previously defined, which justifies the use of notation.

Theorem 6.1. *Let G be a group. For any $a \in G$, $\langle a \rangle$ is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup containing a.*

Proof. Take $a^m, a^n \in \langle a \rangle$. By definition $a^m a^n = a^{m+n} \in \langle a \rangle$, and $(a^n)^{-1} = a^{-n} \in \langle a \rangle$. Therefore $\langle a \rangle$ is a subgroup.

Next, let H be a subgroup containing a. Then $a^n \in H$ for all $n \in \mathbb{Z}$ and therefore $\langle a \rangle \subseteq H$. ■

Theorem 6.2. *Let $G = \langle a \rangle$ be a cyclic group. If the order of G is infinite, then $G \cong (\mathbb{Z}, +)$. If the order of G is n, then $G \cong (Z/n\mathbb{Z}, +)$.*

Proof. Consider the case where the order of G is infinite. Then for all $n \in \mathbb{Z}^+$, $a^n \neq e$. Then for all distinct $n, m \in \mathbb{Z}$, $a^n \neq a^m$. Otherwise, supposing $n > m$, $a^{n-m} = e$ (similarly for $m > n$). Therefore every element of G is uniquely expressed as a^i for some $i \in \mathbb{Z}$. Then the map $\phi : G \to \mathbb{Z}$ defined by $\phi(a^i) = i$ is a bijection. Furthermore

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j)$$

so ϕ is an isomorphism.

Now we consider the case where the order of G is finite. Then there exist some $n \in \mathbb{Z}^+$ such that $a^n = e$, and let n be the smallest one. For all distinct s, t such that $0 \leq s, t < x$, $a^s \neq a^t$. Otherwise, supposing $s > t$, $a^{s-t} = e$, but $0 < s - t < n$ which contradicts the choice of n. Therefore $a^0, a^1, \dots, a^{n-1} \in G$ are distinct and make up all the elements of G. The map $\psi : G \to \mathbb{Z}_n$ defined by $\psi(a^i) = i$ is therefore a bijection. Furthermore

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j)$$

where addition is performed modulo n. Therefore ψ is an isomorphism. ■

7 Cosets

Definition 7.1 (Cosets)**.** Let H be a subgroup of a group G. Let $a \in G$. Then

$$aH = \{ah \mid h \in H\}$$

is the *left coset* of H containing a, and

$$Ha = \{ha \mid h \in H\}$$

is the *right coset* of H containing a. □

The notation can also be extended, i.e. $MN = \{kn \mid m \in M, n \in N\}$ and so on. We will mostly be focusing on left cosets. Theorems and proofs for right cosets are usually very similar.

Theorem 7.1. *Let H be a subgroup of G. Let $a, b \in G$. The following statements are equivalent:*

i. $a^{-1}b \in H$,

ii. $b \in aH$,

iii. $aH = bH$,

iv. $aH \cap bH \neq \emptyset$

Proof.

($i. \implies ii.$): $b = aa^{-1}b \in aH$.

($ii. \implies iii.$): Since $b \in aH$ there exist some $h' \in H$ such that $b = ah'$. Then for any $h \in H$, $bH \ni bh = ah'h \in aH$ so $bH \subseteq aH$. On the other hand, $a = b(h')^{-1}$. This means that $aH \ni ah = b(h')^{-1}h \in bH$. Therefore $aH \subseteq bH$.

($iii. \implies iv.$): If $aH = bH$ but $aH \cap bH = \emptyset$, then $aH = \emptyset = bH$. This is not possible because a group requires at least one element — the identity element e. However $ae \in aH$ so aH cannot be empty.

($iv. \implies i.$): Take $x \in aH \cap bH$. Then there exist $h, h' \in H$ such that $x = ah \in aH$ and $x = bh' \in bH$. This means that

$$\begin{aligned} ah &= bh' \\ h &= a^{-1}bh' \\ a^{-1}b &= h(h')^{-1} \in H \end{aligned}$$

as H is a group. ■

The following shows us that cosets can be thought of as equivalence classes or partitions.

Theorem 7.2. *Let H be a subgroup of G. Define the relation $\sim$ on G as*

$$a \sim b \iff a^{-1}b \in H$$

$\sim$ is an equivalence relation on G.

Proof. $\sim$ is reflexive since $a^{-1}a = e \in H$ as H is a subgroup.

If $a \sim b$, then $a^{-1}b \in H$. Then since H is a subgroup, $(a^{-1}b)^{-1} = b^{-1}a \in H$. Therefore $b \sim a$ and $\sim$ is symmetric.

If $a \sim b$ and $b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$. Therefore, since H is a subgroup, $a^{-1}bb^{-1}c = a^{-1}c \in H$. Therefore $a \sim c$ and $\sim$ is transitive. ■

Lemma 7.3. *Every coset of a subgroup H of a group G has the same order as H.*

Proof. Suppose there exist $h, h' \in H$ such that $gh = gh'$. Then since H is a subgroup, cancellation gives $h = h'$. So the mapping $h \mapsto gh$ is injective. ■

Definition 7.2 (Index)**.** Let H be a subgroup of G. Let $[G : H]$ denote the number of distinct left cosets of H in G. We call this the *index* of H in G. □

Theorem 7.4 (Lagrange's theorem)**.** *Let H be a subgroup of a finite group G. Then, $|H|$ divides $|G|$. Furthermore,*

$$[G : H] = |G|/|H|.$$

Proof. Every coset of H has order $|H|$. However each coset of H is also a partition of G. Therefore $|H|$ divides $|G|$. Next, the cardinality of every coset of H is equal to the cardinality of H. Therefore the number of cosets is equal to $|G|/|H|$. ■

Corollary 7.4.1. *Let H, K be subgroups of G. If $|H|$ and $|K|$ are coprime, then $H \cap K = \{e\}$.*

Proof. Let $J = |H \cap K|$. By Lagrange's theorem, $|J|$ divides both $|H|$ and $|K|$, since J is a subgroup of both $|H|$ and $|K|$. From theorem 1.7, this means that $|J|$ divides $\gcd(|H|, |K|) = 1$, meaning that J only has one element, and this must be the identity. ■

8 Homomorphisms

We have shown some properties regarding homomorphisms in the past. Let us gather all of our facts here:

Theorem 8.1. *Let $\phi : G \to H$ be a group homomorphism. Let e_G and e_H be the identity elements of G and H respectively. Then*

i. $\phi(e_G) = e_H$.

ii. $\forall g \in G\ [\phi(g^{-1}) = (\phi(g))^{-1})]$.

iii. Let G' be a subgroup of G. Then $\phi[G']$ is a subgroup of H.

iv. Let H' be a subgroup of $H \cap \phi[G]$. Then $\phi^{-1}(H')$ is a subgroup of G.

Proof.

i., ii. Theorem 3.1.

iii. Lemma 5.5.

iv. Follows from iii.

■

Theorem 8.2. *If ϕ_1 and ϕ_2 are homomorphisms, then $\phi_1 \circ \phi_2$ is also a homomorphism.*

Proof.

$$\begin{aligned}(\phi_1 \circ \phi_2)(xy) &= \phi_1(\phi_2(xy)) \\ &= \phi_1(\phi_2(x)\phi_2(y)) \\ &= \phi_1(\phi_2(x))\phi_1(\phi_2(y))\end{aligned}$$

■

Definition 8.1 (Kernels)**.** Let $\phi : G \to G'$ be a group homomorphism. The *kernel* of ϕ is defined as

$$\ker \phi = \phi^{-1}[\{e'\}] = \{g \in G \mid \phi(g) = e'\}$$

where e' is the identity element of G'. □

Theorem 8.3. *Let $\phi : G \to G'$ be a group homomorphism. Let $K = \ker \phi$.*

i. K is a subgroup of G.

ii. $\forall k \in K, \forall g \in G,\ [gkg^{-1} \in K]$.

iii. For $g \in G$, $\{g' \in G \mid \phi(g') = \phi(g)\} = gK = Kg$.

Proof. Let e and e' be the identity elements of G and G' respectively.

i. Theorem 8.1.

ii.

$$\begin{aligned}\phi(gkg^{-1}) &= \phi(g)\phi(k)\phi(g^{-1}) \\ &= \phi(g)e'\phi(g)^{-1} \\ &= e'\end{aligned}$$

iii. We can write

$$\begin{aligned}gK &= \{gk \mid \phi(k) = e'\} \\ &= \{gk \mid \phi(gk) = \phi(g)\} \\ &= \{h \in G \mid \phi(h) = \phi(g)\} \\ &= \{kg \mid \phi(k) = e'\} \\ &= Kg.\end{aligned}$$

■

Corollary 8.3.1. *Let $\phi : G \to G'$ be a group homomorphism. ϕ is injective iff $\ker \phi = \{e\}$ where e is the identity element of G.*

Proof. Let $K = \ker\phi$. ϕ is injective iff for every $g \in G$,

$$\{h \in G \mid \phi(g) = \phi(h)\} = gK = \{g\}.$$

This occurs iff $K = \{e\}$. ■

Definition 8.2. Let G and H be two groups and $\phi : G \to H$ be a group homomorphism with kernel K. Define $\mathbf{Sub}(G, K)$ to be the family of all subgroups of G that contains K. Define $\mathbf{Sub}(H)$ to be the family of all subgroups of H. □

Theorem 8.4. *Suppose $\phi : G \to H$ is a surjective homomorphism with kernel K. Define a function $\Phi : \mathbf{Sub}(G, K) \to \mathbf{Sub}(H)$ where $\Phi(G') = \phi[G']$. Then Φ is a bijection.*

Proof. Let $\Phi' : \mathbf{Sub}(H) \to \mathbf{Sub}(G, K)$ be the function defined by $\Phi'(H') = \phi^{-1}[H']$ for $H' \in \mathbf{Sub}(H)$. We will show that Φ' is the inverse function of Φ.

From theorem 8.1, we know that every $\phi^{-1}[H']$ is a subgroup of G. Furthermore, $\phi^{-1}[H']$ contains K since H' contains the identity element, so $\phi^{-1}[H'] \in \mathbf{Sub}(G, K)$.

Next, for $G' \in \mathbf{Sub}(G, K)$, let $G'' = \Phi'(\Phi(G')) = \phi^{-1}[\phi[G']]$. We have $G'' \supseteq G'$ since for any $g \in G'$, $\phi(g) \in \phi[G']$ and so $g \in \phi^{-1}\phi(g) \subseteq \phi^{-1}[G']$. Now take $g'' \in G''$. Then there exists some $g' \in G'$ such that $\phi(g') = \phi(g'')$. By theorem 8.3 we know that $g'' \in g'K$. Since G' contains K, $g'' \in G'$. This shows that $G'' \subseteq G'$, so $G'' = G$. ■

Example 8.1. Let $\phi : \mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$ be defined by $\phi(x) = x \bmod 15$. This is a surjective group homomorphism with kernel $K = 15\mathbb{Z}$. $\mathbf{Sub}(\mathbb{Z}, K) = \{\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}, 15\mathbb{Z}\}$. Then by the theorem above, the images of ϕ on these four elements give all of the subgroups of $\mathbb{Z}/15\mathbb{Z}$. ♢

9 Normal subgroups

Definition 9.1 (Normal subgroups)**.** Let G be a group and N be a subgroup of G. We call N a *normal* subgroup if

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

□

In any group, the group itself and the set containing the identity element itself are the two trivial normal subgroups.

Theorem 9.1. *The kernel of a group homomorphism is a normal subgroup.*

Proof. This follows immediately from theorem 8.3. ■

Example 9.1. Let G be a group. Define

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

Z is also known as the *centre* of G. Z is a normal subgroup of G.

First of all, Z is a subgroup. Take any $y, z \in Z$ and $g \in G$. Then

$$zyg = zgy = gzy$$

so $zy \in Z$. Next

$$z^{-1}g = z^{-1}gzz^{-1} = z^{-1}zgz^{-1} = gz^{-1}$$

so $z^{-1} \in Z$.

Z is a normal subgroup since for any $z \in Z$ and $g \in G$, if $zg = gz$ then $z = gzg^{-1} \in Z$. $\lozenge$

Theorem 9.2. *If G is an abelian group then every subgroup of G is normal.*

Proof. Let N be a subgroup of G and take $n \in N$ and $g \in G$. Since G is abelian,

$$gng^-1 = gg^-1n = n \in N.$$

■

Theorem 9.3. *Let H be a subgroup of G. Take any $g, g' \in G$. The following statements are equivalent:*

i. H *is a normal subgroup.*

ii. $gHg^{-1} = H$.

iii. $gH = Hg$.

iv. $(gH)(g'H) = (gg')H$.

Proof.

($i. \implies ii.$): For all $ghg^{-1} \in gHg^{-1}$, $ghg^{-1} \in H$ so $gHg^{-1} \subseteq H$. For all $h \in H$ and $g \in G$, $g^{-1}hg \in H$, which means $g(g^{-1}hg)g^{-1} \in gHg^{-1}$ and so $H \subseteq gHg^{-1}$.

($ii. \implies iii.$): $gH = gH(g^{-1}g) = (gHg^{-1})g = Hg$.

($iii. \implies iv.$): $gHg'H = gg'HH = gg'H$.

($iv. \implies i.$): For any $h \in H$ and $g \in G$, we have $(gh)(g^{-1}e) \in gg^{-1}H = H$. ■

Theorem 9.4. *Let H_1 and H_2 be two groups and let $H_1 \times H_2$ be its product group. Let $\phi_1 : G \to H_1$ and $\phi_2 : G \to H_2$ be group homomorphisms. Then $\phi_G \to H_1 \times H_2$ given by $\phi(g) = (\phi_1(g), \phi_2(g))$ is also a group homomorphism.*

Proof.

$$\begin{aligned}
\phi(gg') &= (\phi_1(gg'), \phi_2(gg')) \\
&= (\phi_1(g)\phi_1(g'), \phi_2(g)\phi_2(g')) \\
&= (\phi_1(g), \phi_2(g))(\phi_1(g'), \phi_2(g')) \\
&= \phi(x)\phi(y)
\end{aligned}$$

■

9.1 Simple groups

Definition 9.2 (Simple groups)**.** A group G is called *simple* if its only normal subgroups are the trivial subgroups $\{e\}$ and G. □

Example 9.2. Let p be a prime number. Then $G = \mathbb{Z}/p\mathbb{Z}$ is a simple group. By Lagrange's theorem the order of any subgroup H of G must divide the order of G. This then means $|H|$ is either 1 or p. ♢

10 Quotient groups

Definition 10.1 (Quotient groups)**.** Let H be a normal subgroup of G. Then the set of left cosets of H, written G/H, with the binary operation $*$ defined as

$$\forall g_1H, g_2H \in G/K,\ [g_1K * g_2K = g_1g_2K].$$

is known as a *quotient group* of G mod H.

We write $H\backslash G$ to denote the set of right cosets of H. Again with the appropriate binary operation this also forms a group. □

Theorem 10.1. *Let H be a normal subgroup of G. $(G/H, *)$ forms a group.*

Proof. Take any $g, g_1, g_2, g_3 \in G$. We check the group axioms.

G1. $*$ is indeed a binary operation.

G2. From theorem 9.3,

$$\begin{aligned} g_1H * (g_2H * g_3H) &= g_1Hg_2g_3H \\ &= g_1g_2g_3H \\ &= g_1g_2H * g_3H \\ &= (g_1H * g_2H) * g_3H \end{aligned}$$

G3. Take the identity element e of G. Then the identity element of G/H is $eH = H$:

$$gH * eH = gH \qquad eH * gH = gH$$

G4. Given gH, its inverse is $g^{-1}H$:

$$gH * g^{-1}H = eH \qquad g^{-1}H * gH = eH$$

■

Theorem 10.2. *Let G be an infinite cyclic group. Then every quotient group of G except $G/\{e\}$ is finite.*

Proof. Infinite cyclic groups are isomorphic to $\mathbb{Z}$ (theorem 6.2). Any subgroup of G is a normal subgroup since it is abelian (theorem 9.2). Furthermore any subgroup of $\mathbb{Z}$ takes the form of $d\mathbb{Z}$ (theorem 4.2). Therefore for any subgroup N of G, $G/N \cong \mathbb{Z}/dZ$ which is finite. ■

Theorem 10.3. *Let H be a normal subgroup of G. The function $\gamma : G \to G/H$ defined by $\gamma(x) = xH$ is a homomorphism with kernel H.*

Proof. For all $x, y \in G$,

$$\gamma(xy) = (xy)H = (xH)(yH) = \gamma(x)\gamma(y)$$

so γ is a homomorphism. Next, since $xH = eH$ iff $x \in H$. Therefore $\ker \gamma = H$. ■

γ is also known as the *natural homomorphism* and sometimes as the *quotient map*.

Theorem 10.4 (Fundamental/first homomorphism theorem)**.** *Let $\phi : G \to G'$ be a group homomorphism with kernel K. Let $\gamma : G \to G/K$ be the natural homomorphism. Then $\mu : G/K \to \phi[G]$ given by $\mu(gK) = \phi(g)$ is a well-defined group isomorphism and $\phi = \mu\gamma$.*

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\gamma"'] & & \phi[G] \\
& G/K \arrow[ur, "\mu", "\cong"'] &
\end{tikzcd}$$

Proof. Theorem 8.3 tells us that for any $g \in G$, $gK = \{x \in G \mid \phi(x) = \phi(g)\}$.

μ is injective, since if $\phi(g_1) = \phi(g_2)$, then from the above statement, this would mean that $g_1 \in g_2K$ and $g_1K = g_2K$. It is also surjective on its own domain. Finally, μ is a homomorphism since

$$\begin{aligned}
\mu(g_1Kg_2K) &= \mu((g_1g_2)K) \\
&= \phi(g_1g_2) \\
&= \phi(g_1)\phi(g_2) \\
&= \mu(g_1K)\mu(g_2K).
\end{aligned}$$

Lastly, it is straightforward that $\phi(g) = \mu\gamma$. ■

Example 10.1. Let $\phi : (\mathbb{Z}, +) \to (\mu_n, \times)$ be the surjective group homomorphism given by $\phi(k) = \exp\left(\frac{2k\pi i}{n}\right)$. Then $\ker \phi = n\mathbb{Z}$ and we have a group isomorphism $\mu : \mathbb{Z}/n\mathbb{Z} \to \mu_n$ defined by $\mu(k + n\mathbb{Z}) = \exp\left(\frac{2k\pi i}{n}\right)$. ♢

Example 10.2. Let $T = \{z \in \mathbb{C} \mid |z| = 1\}$ (the circle group) be the unit circle in the complex plane. Then $(T, \times)$ is a subgroup of $(\mathbb{C}, \times)$. Consider the surjective homomorphism $\phi : (\mathbb{R}, +) \to (T, \times)$ given by $\phi(x) = \exp(2\pi ix)$. Its kernel is $\mathbb{Z}$. The first isomorphism theorem then gives us an isomorphism $\mu : (\mathbb{R}/\mathbb{Z}, +) \to (T, \times)$ given by $\mu(x + \mathbb{Z}) = \exp(2\pi ix)$. ♢

Example 10.3. Consider the surjective group homomorphism $\phi : (\mathbb{C}, \times) \to (\mathbb{R}, +)$ given by $\phi(z) = |z|$. Its kernel is the complex unit circle, T (see above). A coset zT is a circle centred around the origin but with radius $|z|$. The quotient group $\mathbb{C}/T$ is then the set of all circles in $\mathbb{C}$ centred at the origin with positive radius. The first isomorphism theorem gives an isomorphism $\mu : \mathbb{C}/T \to \mathbb{R}$. It maps the circle zT to its radius $|z|$. ♢

Corollary 10.4.1. *Let $\phi : G \to G'$ and $\psi : G \to G''$ be two group homomorphisms with the same kernel K. Then $\phi[G] \cong \psi[G]$, and furthermore, if G is a finite group, then*

$$|\phi[G]| = |\psi[G]| = |G/K| = |G|/|K|.$$

Proof. By the first isomorphism theorem, $\phi[G] \cong G/K$ and $\psi[G] \cong G/K$. Therefore $\phi[G] \cong \psi[G]$. If G is finite then the second statement follows immediately from this fact. ■

Before we state the second isomorphism theorem we will cover two quick facts.

Theorem 10.5. *Let G be a group. Let M be a subgroup of G and let N be a normal subgroup of G. Then $MN = NM$ and it is a subgroup of G.*

Proof. Let $m \in M$ and $n \in N$. Then $mn = (mnm^{-1})m \in NM$ since $mnm^{-1} \in N$ as it is normal. Similarly, $nm = m(m^{-1}nm) \in MN$. Thus $MN = NM$.

Next we show that MN is a subgroup. Pick $m_1n_1, m_2n_2 \in MN$. Then

$$\begin{aligned} m_1n_1(m_2n_2)^{-1} &= m_1n_1n_2^{-1}m_2^{-1} \\ &= (m_1m_2^{-1})(m_2n_1n_2^{-1}m_2^{-1}) \in MN \end{aligned}$$

■

Since MN contains N as a normal subgroup, this means the quotient group MN/N is well defined. It is also important that N is normal.

Theorem 10.6. *Let G be a group. Let M be a subgroup of G and let N be a normal subgroup of G.*

i. The function $\phi : M \to MN/N$ defined by $\phi(m) = mN$ is a surjective group homomorphism.

ii. The kernel of ϕ is $M \cap N$, which is a normal subgroup of M.

Proof.

i. First we note that

$$MN/N = \{mnN \mid m \in M, n \in N\} = \{mN \mid m \in M\}.$$

Therefore ϕ is a surjection. Next, for any $x, y \in M$,

$$\phi(x)\phi(y) = xNyN = xyNN = \phi(xy)$$

using the fact that $yN = Ny$ (theorem 9.3). So ϕ is also a homomorphism.

ii. If $m \in \ker\phi$ then $\phi(m) = mN = N$, which means $m \in N$. Therefore, $m \in M \cap N$. Conversely if $m \in M \cap K$ we have $\phi(m) = mN = N$, so $m \in \ker\phi$. The kernel of a homomorphism is a normal subgroup.

■

Theorem 10.7 (Second isomorphism theorem)**.** *Let G be a group. Let M be a subgroup of G and let N be a normal subgroup of G. Then we have*

$$M/(M \cap N) \cong (MN)/N.$$

Proof. The previous theorem defines a surjective group homomorphism $\phi : M \to MN/N$. Then the first isomorphism theorem tells us that MN/N is isomorphic to $M/\ker\phi = M/(M\cap N)$. ■

Theorem 10.8 (Third isomorphism theorem)**.** *Let G be a group. Let M and N be normal subgroups of G such that $M \supseteq N$. Then M/N is a normal subgroup of G/N and*

$$(G/N)/(M/N) \cong G/M$$

Proof. We define $\phi : G/N \to G/M$ by $\phi(gN) = gM$.

First of all, ϕ is well defined. If $g_1N = g_2N$, then $g_1 = g_2n$ for some $n \in N$, and

$$\phi(g_1N) = g_1M = g_2nM = g_2M = \phi(g_2N).$$

Next, ϕ is a homomorphism since

$$\begin{aligned}\phi(g_1Ng_2N) &= \phi(g_1g_2N)\\ &= g_1g_2M\\ &= g_1Mg_2M\\ &= \phi(g_1N)\phi(g_2N).\end{aligned}$$

ϕ is also surjective since for all $gM \in G/M$, $\phi(gN) = gM$.

Furthermore, $\ker\phi = M/N$. If $\phi(gN) = gM = e_{G/M} = M$, then $g \in M$. Therefore $gN \in M/N$. Conversely if $gN \in M/N$ where $g \in M$, then $\phi(gN) = gM = M$. Therefore $gn \in \ker\phi$. Note that this implies that M/N is a normal subgroup.

Finally, we apply the first isomorphism theorem. Since $\phi : G/N \to G/M$ is a surjective homomorphism,

$$G/M \cong (G/N)/\ker\phi = (G/N)/(M/N)$$

■

Example 10.4. Consider $\mathbb{Z}$, $5\mathbb{Z}$, and $10\mathbb{Z}$:

$$(\mathbb{Z}/10\mathbb{Z})/(5\mathbb{Z}/10\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z}).$$

◊

11 Euler's totient function

This section is mainly an application of group theory to number theory. Euler's totient function, $\varphi(n)$ gives the multitude of coprime numbers less than n. Now, define a set

$$\Phi(n) = \{x \in \mathbb{Z} \mid 0 \leq x \leq n, \gcd(x, n) = 1\}.$$

So $\varphi(n) = |\Phi(n)|$.

Let operation $*_n$ denote multiplication modulo n. We will also have to differentiate between ordinary exponentiation x^k and exponentiation with $*_n$ as $x^{*_n,k}$.

Theorem 11.1. *$(\Phi(n), *_n)$ is a group.*

Proof. We check the axioms again:

G1. Take any $x, y \in \Phi(n)$. This means $\gcd(x, n) = \gcd(y, n) = 1$. This means that there exists integers a, b, c, d such that $ax + bn = cy + dn = 1$. Furthermore, there exists some integer k such that $kn = xy - (x * y)$. Then,

$$\begin{aligned} 1 &= (ax + bn)(cy + dn) \\ &= acxy + adxn + bcyn + bdnn \\ &= ac(xy - kn) + (adx + bcy + bdn + ack)n \end{aligned}$$

which means that $\gcd(x * y, n) = 1$.

G2. For any $x, y, z, \in \Phi(n)$,

$$\begin{aligned} (x * y) * z &\equiv xy * z \pmod n \\ &\equiv xyz \pmod n \\ &\equiv x(y * z) \pmod n \\ &\equiv x * (y * z). \end{aligned}$$

G3. 1 is the identity element.

G4. Let $x \in \Phi(n)$. Since $\gcd(x, n) = 1$, there exists integers a, b such that $ax + bn = 1$. By the Euclidean algorithm, there exists some q, x' with $0 \leq x' < n$ such that $a = qn + x'$. Then

$$\begin{aligned} 1 &= ax - qnx + bn + qnx \\ &= x'x + (b + qx)n \end{aligned}$$

which means that $\gcd(x', n) = 1$ and so $x' \in \Phi(n)$. Also, $x'x \equiv 1 \pmod n$ so $x' * x = 1$.

■

Theorem 11.2 (Euler's theorem)**.** *Let x be an integer coprime to n. Then*

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

Proof. First let $y \in \Phi(n)$. Suppose y has order o, i.e. $y^{*,o} = 1$. Consider the cyclic subgroup $\langle y \rangle$. By Lagrange's theorem, $|\langle y \rangle| = o$ divides $|\Phi(n)| = \varphi(n)$. This means there exist some integer d such that $\varphi(n) = do$ and so

$$y^{*,\varphi(n)} = y^{*,o*,d} = 1^{*,d} = 1.$$

We can perform induction to show that $y^k = y^{*,k} \pmod n$, which we skip. This combined with the above gives us

$$y^{\varphi(n)} \equiv y^{*,\varphi(n)} = 1 \pmod n.$$

Now let x be an integer such that $\gcd(x, n) = 1$. By the Euclidean algorithm there exists integers q, r, such that $x = qn + r$ with $0 \leq r < n$, and $\gcd(n, r) = \gcd(x, n) = 1$. Therefore $r \in \Phi(n)$, so from the previous paragraph we get that

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

■

Next we will discuss some of the properties of the totient function.

It is quite clear that if p is a prime, then $\varphi(p) = p = 1$ and $Phi(p)$ would be the set of numbers from 1 to $p-1$. More generally, consider the power of a prime $n = p^r$. Take $x \in \Phi(n)$. $\gcd(x, p^r) = 1$ iff p does not divide x. Therefore $\Phi(n)$ is the set of numbers from 0 to $n-1$ excluding the multiples of p. There are $\frac{n}{p}$ multiples, so

$$\varphi(n) = n - \frac{n}{p} = p^{r-1}(p-1).$$

Using Euler's theorem, if $p \nmid x$, then

$$x^{\varphi(p^r)} = x^{p^{r-1}(p-1)} \equiv 1 \pmod{p^r}.$$

Specifically when $r = 1$ we get Fermat's little theorem:

$$x^{p-1} \equiv 1 \pmod{p}.$$

Next, for two coprime m, n, $\varphi(mn) = \varphi(m)\varphi(n)$. The Chinese remainder theorem gives an isomorphism $F : \mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ given by $F(x) = (x \bmod m, x \bmod n)$. Therefore there is also a bijection from $\Phi(mn) \to \Phi(m) \times \Phi(n)$. Counting elements give us the original claim.

With these two results, we can see that for any integer n with prime factorization $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$,

$$\varphi(n) = \varphi(p_1^{r_1})\varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}).$$

12 Automorphism groups

Definition 12.1 (Automorphisms). Let $(G, *)$ be a group. An isomorphism $\phi : G \to G$ is called an *automorphism*.

Denote the set of automorphisms of G as $\mathrm{Aut}(G)$. □

Theorem 12.1. $(\mathrm{Aut}(G), \circ)$ *forms a group where* $\circ$ *is composition.*

Proof. We have shown some of these results in the past (theorem 3.2).

G1. Isomorphisms are closed under composition.

G2. Composition is associative.

G3. The identity map is in $\mathrm{Aut}(G)$.

G4. The inverse of an isomorphism is also an isomorphism.

■

Definition 12.2 (Automorphism groups). The group $(\mathrm{Aut}(G), \circ)$ is called the *automorphism* group of G. □

We give examples of some automorphisms.

Example 12.1. Let G be a group and let $g \in G$, then $\phi_g(x) : G \to G$ defined by $\phi_g(x) = gxg^{-1}$ is known as an *inner automorphism* of G.

We can see that ϕ_g is a bijection since its inverse function is $\phi_{g^{-1}}$. It is also a homomorphism since

$$\phi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y).$$

◊

Theorem 12.2. *The set* $\mathrm{Inn}(G)$ *of all inner automorphisms is a normal subgroup of* $\mathrm{Aut}(G)$.

Proof. First we establish that $\mathrm{Inn}(G)$ is a subgroup. Given $\phi_f, \phi_g \in \mathrm{Inn}(G)$,

$$(\phi_f\phi_g)(x) = fgxg^{-1}f^{-1} = \phi_{fg}(x).$$

So $\mathrm{Inn}(G)$ is closed. Next $\phi_g\phi_{g^{-1}} = \phi_{g^{-1}}\phi_g = \phi_e$ the identity element. We skip the checking. This shows that $\mathrm{Inn}(G)$ is a subgroup.

Let $\sigma \in \mathrm{Aut}(G)$. Then for all $x \in G$,

$$(\sigma\phi_g\sigma^{-1})(x) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)x\sigma(g)^{-1} = \phi_{\sigma(g)}(x).$$

Therefore $\sigma\phi_g\sigma^{-1} \in \mathrm{Inn}(G)$. ■

Theorem 12.3. *The map* $T : G \to \mathrm{Inn}(G)$ *given by* $T(g) = \phi_g$ *is a surjective group homomorphism whose kernel is the centre of the group* G.

Proof. T is clearly surjective. It is a homomorphism since

$$T(gg') = \phi_{gg'} = \phi_g\phi_{g'} = T(g)T(g')$$

as we have shown previously. Finally,

$$\begin{aligned} g \in \ker T &\iff T(g) = \mathrm{id}_G \\ &\iff \forall x \in G\ (\phi(x) = x) \\ &\iff \forall x \in G\ (gxg^{-1} = x) \\ &\iff \forall x \in G\ (gx = xg) \end{aligned}$$

■

13 The Sylow theorems

TODO