MA2202

- To prove uniqueness, suppose not unique and try to show equality.
- To prove equality of two sets, show that each is a subset of the other.
- To show that two groups are not isomorphic, prove by contradiction.
- Element x has finite order $\implies x^a = e$ for some a
- Intersection with $A_n \implies$ only take even permutations, which have $\text{sgn}(x) = 1$.

Functions

Let A, B be sets, and let $f : A \to B$ be a function.

- For $a \in A$, denote $f(a) = b \in B$.
- The set A is called the domain, and the set B is called the co-domain.
- The range/image of f is
$$\{b \in B : b = f(a) \text{ for some } a \in A\}$$
- Let $B' \subseteq B$. Define
$$f^{-1}(B') = \{a \in A : f(a) \in B'\}$$
- If $g : C \to D$ is another function, then we say $f = g \iff A = C, B = D$ and $f(a) = g(a)\ \forall a \in A$
- If $S \subseteq A$, then $f|_S$ denotes the same function except that the domain A is replaced by S. This function $f|_S$ is called the restriction of f to S.
- If $h : B \to C$, then the composite of h and f is a function $h \circ f : A \to C$ given by
$$(h \circ f)(a) = h(f(a)) \quad \forall a \in A$$

Notable examples

- The identity fn on A is $f : A \to A$ defined by
$$f(x) = x \quad \forall x \in A$$
We also denote the identity function on A by id_A.
- The inclusion fn on Y for some $Y \subset X$ is the function $h : Y \to X$ defined by $h(y) = y\ \forall y \in Y$.

Injection/Surjection/Bijection Let $f : A \to B$ be a function.

1. f is an injection if $f(a) = f(a') \implies a = a'$.
2. f is a surjection if $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$.
3. f is a bijection if it is both an injection and a surjection.
4. If f is a bijection, we can define the inverse function $f^{-1} : B \to A$ in the following way: $\forall b \in B, \exists$ unique $a \in A$ such that $f(a) = b$. Then $f^{-1}(b) = a$.
5. A fn is a bijection $\iff$ its inverse fn exists.

Integers

Divisibility

Given $a, b \in \mathbb{Z}$ where $a \neq 0$.

- We say a divides b if $b = ma$ for some $m \in \mathbb{Z}$. The integer b is a multiple of a, and we write $a|b$.
- An integer n is called a unit if it divides 1. Hence $n = 1$ or -1.
- Transitivity holds, i.e. $a|b$ and $b|c \implies a|c$

Prime

A nonzero $p \in \mathbb{Z}$ is called a prime integer if:

1. p is not a unit (i.e $p \neq \pm 1$), and
2. if p divides ab for some $a, b \in \mathbb{Z}$, then $p|a$ or $p|b$.

A positive prime integer is called a prime number.

Irreducible

A nonzero $p \in \mathbb{Z}$ is called a irreducible integer if:

1. p is not a unit (i.e $p \neq \pm 1$), and
2. if p divides xy for some $x, y \in \mathbb{Z}$, then either x or y is a unit, i.e. x or y is ± 1.

Prime vs irreducible

Let p be an integer. It is an irreducible integer $\iff$ it is a prime integer.

The Euclidean algorithm

Let $x, y \in \mathbb{Z}$ with $y \neq 0$. Then there exist unique integers q and r such that
$$x = qy + r \text{ and } 0 \leq r < |y|$$
This is also known as the division algorithm.

Common divisor

Given two integers x and y where $y \neq 0$.

- A nonzero integer m is called a common divisor if $m|x$ and $m|y$.
- 1 is always a common divisor.
- If m is a common divisor, $-m$ is also a common divisor.
- Every common divisor lies bewtween $-|y|$ and $|y|$.
- There are only finitely many common divisors.

Greatest common divisor

There is a largest number d among the common divisors of x and y, which we call the GCD of x and y. Denote it by $d = \gcd(x, y)$.

- Since 1 is always a common factor, $d \geq 1$
- $\gcd(0, y) = |y|$
$$\gcd(x, y) = \gcd(y, x) = \gcd(x, |y|) = \gcd(|x|, y) = \gcd(|x|, |y|)$$
- $\gcd(cx, cy) = |c| \gcd(x, y)$
- $\gcd(x, y) = \gcd(x + y, y) = \gcd(x - y, y)$

Connection with Euclidean algorithm Let x, y be integers where $y \neq 0$. Let $x = qy + r$ where $0 \leq r < |y|$. Then
$$\gcd(x, y) = \gcd(y, r)$$

Computing GCD

Given $x_1, x_2 \in \mathbb{Z}$. If $x_2 = 0$, then $\gcd(x_1, x_2) = |x_1|$. Else, $x_2 \neq 0$.
Assume $x_2 \neq 0$. Since $\gcd(x_1, x_2) = \gcd(x_1, |x_2|)$, suppose $x_2 > 0$. By the division algorithm,
$$x_1 = qx_2 + x_3 \quad \text{for some } 0 \leq x_3 < x_2$$
By the lemma above,
$$\gcd(x_1, x_2) = \gcd(x_2, x_3)$$
Doing this repeatedly, we get
$$\gcd(x_1, x_2) = \gcd(x_2, x_3) = \cdots = \gcd(x_m, 0) = x_m$$
where $|x_2| > x_3 > x_4 > \cdots \geq 0$.

Example $\gcd(6804, -930) = \gcd(6804, 930)$.
$$\begin{aligned} 6804 &= 7(930) + 294 \\ 930 &= 3(294) + 48 \\ 294 &= 6(48) + 6 \\ 48 &= 8(6) + 0 \end{aligned}$$
Hence,
$$\gcd(6804, -930) = \gcd(6804, 930) = \gcd(930, 294) = \gcd(294, 48) = \gcd(48, 6) = \gcd(6, 0) = 6$$
Then, by reverse engineering,
$$\begin{aligned} 6 &= 294 - 6(48) \\ &= 294 - 6(930 - 3(294)) \\ &= -6(930) + (19)(294) \\ &= -6(930) + (19)(6804 - 7(930)) \\ &= 19(6804) - 139(930) \\ &= (19)(6804) + 139(-930) \end{aligned}$$
Hence, $6 = a(6804) + b(-930)$ for some $a, b \in \mathbb{Z}$.

Proposition Let $d = \gcd(x, y)$ where $y \neq 0$. Then

1. We have $d = ax + by$ for some $a, b \in \mathbb{Z}$
2. Let $I = \{mx + ny \in \mathbb{Z} : m, b \in \mathbb{Z}\}$. Then $I = d\mathbb{Z}$ is the set of all the multiples of d.
3. If an integer c divides both x and y, then c divides d.

GCD of 3 or more integers

Let $x, y, z \in \mathbb{Z}$, and not all are 0. We say c is a common divisor of x, y, z if c divides x, y, z. The GCD of x, y, z is denoted by $d = \gcd(x, y, z)$.

1. If c divides x, y, z then c divides $\gcd(x, y)$ and z.
2. $\gcd(x, y, z) = \gcd(\gcd(x, y), z)$
3. $d = mx + ny + pz$ for some $m, n, p \in \mathbb{Z}$
4. $I = \{mx + ny + pz : m, n, p \in \mathbb{Z}\} = d\mathbb{Z}$

Tut 1 Q2 (GCD given prime factorization)

Suppose
$$x = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}, y = p_1^{f_1} p_2^{f_2} \cdots p_s^{f_s}$$
$$d = p_1^{g_1} p_2^{g_2} \cdots p_s^{g_s}$$
are prime factorizations of x, y, d, with p_i being distinct positive prime integers, and $e_i, f_i, g_i \geq 0$. Then

- The integer d divides $x \iff g_i \leq e_i$ for all i.
- If $d|x$ and $d|y$, then $g_i \leq \min\{e_i, f_i\}$ for all i.
- GCD is
$$\gcd(x, y) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_s^{\min\{e_s, f_s\}}$$
- If $d|x$ and $d|y$, then $d|\gcd(x, y)$

The fundamental theorem of arithmetic

Let $n > 1$ be a positive integer. Then there exists a factorization
$$n = p_1 p_2 \cdots p_s$$
where p_i is a (positive) prime number for all i, and $p_1 \leq p_2 \leq \cdots \leq p_s$. This factorization is unique.

Mathematical induction

Let $P(1)$ be a property that depends on $n \in \mathbb{N}$. If

1. $P(1)$ holds and
2. if $P(k)$ holds, then $P(k + 1)$ holds

then $P(n)$ holds $\forall n \in \mathbb{N}$.

Strong MI

Let $P(1)$ be a property that depends on $n \in \mathbb{N}$. If

1. $P(1)$ holds and
2. if $P(i)$ holds for $1 \leq i \leq k$, then $P(k + 1)$ holds

then $P(n)$ holds $\forall n \in \mathbb{N}$.

Binomial theorem

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \quad \forall n \in \mathbb{N}$$

Fermat's little theorem

Let p be a prime number. Then
$$p|(n^p - n) \quad \forall n \in \mathbb{Z}$$
i.e.
$$n^p \equiv n \pmod{p} \implies n^{p-1} \equiv 1 \pmod{p}$$
Applying this idea,
$$n^{a(p-1)+b} \equiv n^b \pmod{p}$$

Equivalence relations

Relation

Let A be a set. A subset R of $A \times A$ is a relation on A. For $a, b \in A$, $a \sim b \iff (a, b) \in R$. We may write it as $a \sim_R b$.

Equivalence relation

Let A be a set. A relation R on A (i.e. $R \subseteq A \times A$) is an equivalence relation on A if for all a, b, c,

- (E1) $a \sim a$ (reflexive)
- (E2) $a \sim b \implies b \sim a$ (symmetric)
- (E3) $a \sim b \wedge b \sim c \implies a \sim c$ (transitive)

Equivalence class

Let R be an equivalence relation on a set A. Let $a \in A$. The equivalence class of $a \in A$ is the subset
$$\{x \in A : a \sim x\}$$
and we denote it by $Cl(a)$.

Partition

Let A be a set and let $\{A_i : i \in I, A_i \subseteq A\}$ be a collection of subsets of A. We say that the collection $\{A_i : i \in I\}$ forms a partition of A if

- (P1) $A = \bigcup_{i \in I} A_i$, and
- (P2) $A_i \cap A_j = \emptyset$ for all $i, j \in I$ and $i \neq j$

Alternatively, P2 can be stated as: If $A_i \cap A_j$ is a nonempty subset, then $A_i = A_j$.

Collection of all equivalence classes

Let R be an equivalence relation on a set A. The set of equivalence classes $\{Cl(a) : a \in A\}$ is denoted by A/R, $A/\sim_R$, or simply $A/\sim$.

- The collection of all equivalence classes forms a partition of A.
- The map $p : A \to A/R$ given by $p(a) = Cl(a)$ is called the quotient map.

Linear Congruences

Congruent modulo m

Let m be a positive integer. Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{m}$ if $m|(a - b)$.

- $\equiv$ is an equivalence relation on $\mathbb{Z}$.
- If $x \equiv y \pmod{m}$ and $z \equiv w \pmod{m}$, then $x + z \equiv y + w \pmod{m}$ and $xz = yw \pmod{m}$.

Simultaneous congruence equations

Solution to congruence equation

Suppose $\gcd(a,m)=1$. For $b\in\mathbb{Z}$, the congruence equation
$$ax\equiv b \pmod m$$
has a solution $x\in\mathbb{Z}$, that is unique modulo m, i.e. $x'\in\mathbb{Z}$ is another solution iff
$$x\equiv x' \pmod m$$

Solving We can find a solution by writing $1=az+my$, then $b=b(az+my)$, then $b\equiv a(bz) \pmod m$. Then bz is a solution.

Chinese Remainder Theorem

Suppose $\gcd(m,m')=1$. Then the congruence equations
$$x\equiv b \pmod m$$
$$x\equiv b' \pmod{m'}$$
have a common solution $x\in\mathbb{Z}$, that is unique modulo mm', i.e. if $x'\in\mathbb{Z}$ is another solution, then
$$x\equiv x' \pmod{mm'}$$

Solving simultaneous congruence equations

Solve the simultaneous congruence equations
$$x\equiv 3 \pmod{13}$$
$$x\equiv 5 \pmod{11}$$
By the division algorithm, we have $13=11+2$ and $11=5(2)+1$. Hence,
$$\begin{aligned}\gcd(13,11)&=1=11-5(2)\\&=11-5(13-11)=-5(13)+6(11)\end{aligned}$$
This implies
$$6(11)\equiv 1 \pmod{13}$$
$$-5(13)\equiv 1 \pmod{11}$$
Consider $x=5(-5)(13)+3(6)(11)=-127$. We can show that this is a solution, and then by the Chinese Remainder Theorem, all solutions are of the form $x=-127+k(13)(11)$.

Binary operations

Definition

Let G be a set. A binary op $*$ on G is a function
$$*:G\times G\to G$$

- For $(x,y)\in G$, we denote $*(x,y)$ by $x*y$.
- Associative if $\forall a,b,c\in G$, $(a*b)*c=a*(b*c)$.
- Commutative/abelian if $\forall a,b\in G$, $a*b=b*a$.

Multiplication table

Let $G=\{a,b,c\}$. We can represent a binary operation $*$ with a multiplication table:

$x*y$	$y=a$	b	c
$x=a$	a	a	b
b	a	c	c
c	b	a	c

For $*$ to be abelian, the multiplication table should be symmetric along the diagonal. In this case, $*$ is not abelian because $b*c=c$ but $c*b=a$.

Identity

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

- e is a left identity element if $\forall a\in G$, $e*a=a$.
- e is a right identity element if $\forall a\in G$, $a*e=a$.
- e is an identity element if $\forall a\in G$, $e*a=a*e=a$.

Groups

Group axioms

A group $(G,*)$ consists of a set G and a binary operation $*$ on G which satisfies four axioms:

- (G1) (Closure) For all $a,b\in G$, $a*b\in G$.
- (G2) (Associativity) For all $a,b,c\in G$,
$$(a*b)*c=a*(b*c)$$
- (G3) (Existence of identity element) $\exists e\in G$ such that for all $a\in G$,
$$e*a=a*e=a$$
Note that the identity element is unique.
- (G4) (Existence of inverse element) For each $a\in G$, $\exists b\in G$ such that
$$a*b=b*a=e$$
where e is the identity element in (G3). Note that the inverse of an element is unique.

Order

The number of elements in G is called the order of G. We denote it by $|G|$. If $|G|$ is finite, then we call G a finite group. Otherwise it is an infinite group.

Abelian group

A group $(G,*)$ is called an abelian group if $a*b=b*a$ for all $a,b\in G$.

Some theorems

Let $(G,*)$ be a group. Let $a,b,c\in G$. Then

- $(a^{-1})^{-1}=a$
- $(a*b)^{-1}=b^{-1}*a^{-1}$
- $a^{-1}*\cdots*a^{-1}=(a*\cdots*a)^{-1}$ where there are n copies of a^{-1} and a on both sides.
- (Cancellation Law) If $a*c=b*c$, then $a=b$. If $c*a=c*b$, then $a=b$.
- Given $a,b\in G$, the equation $a*x=b$ (and respectively $x*a=b$) has a unique solution $x\in G$.
- $a^n*a^m=a^{n+m}$ for $n,m\in\mathbb{Z}$.

Weakened axioms

For (G3) and (G4), if we show either

- just right identity + right inverse,
- or just left identity + left inverse,

and if (G1) and (G2) are already proven, then we have a group.

Product group

Let $(G,*)$ and $(H,\star)$ be two groups. Consider the Cartesian product $G\times H=\{(g,h):g\in G,h\in H\}$. Define binary operation $\cdot$ on $G\times H$ by
$$(g,h)\cdot(g',h')=(g*g',h\star h')$$
for all $(g,h),(g',h')\in G\times H$. Then $(G\times H,\cdot)$ forms a group, called the product group of $(G,*)$ and $(H,\star)$.

- Identity element is (e_G,e_H) where e_G and e_H are the identity elements of G and H respectively.
- Inverse element of (g,h) is (g^{-1},h^{-1}).

Group isomorphisms

Definition

Let $(G,*)$ and $(H,\star)$ be two groups. We say that these two groups are isomorphic if there exists a bijection $\phi:G\to H$ such that
$$\phi(g_1*g_2)=\phi(g_1)\star\phi(g_2)$$
for all $g_1,g_2\in G$.

- The bijection ϕ is called a group isomorphism.
- We denote $(G,*)\simeq(H,\star)$ and $\phi:(G,*)\xrightarrow{\sim}(H,\star)$.
- If $(G,*)$ and $(H,\star)$ are isomorphic finite groups, then they have the same order.
- If $(G,*)$ is an abelian group, then $(H,\star)$ is an abelian group.
- $\phi:G\to G$ given by $\phi(g)=g^{-1}$ is a group isomorphism $\iff$ G is an abelian group.

Two isomorphisms

Suppose $\phi:(G,*)\to(H,\star)$ and $\psi:(H,\star)\to(K,\cdot)$ are two isomorphisms of groups. Then

- the inverse function $\phi^{-1}:(H,\star)\to(G,*)$ and
- the composite function $\psi\circ\phi:(G,*)\to(K,\cdot)$

are group isomorphisms.

Subgroups

Definition

Let $(G,*)$ be a group. Let $H\subseteq G$ be a nonempty subset. Suppose $(H,*)$ forms a group, i.e. it satisfies the four group axioms. Then $(H,*)$ is called a subgroup of $(G,*)$. Note that the binary operation is the same for G and H.

Integer multiple Suppose $(I,+)$ is a subgroup of $(\mathbb{Z},+)$. Then $I=d\mathbb{Z}$ for some integer $d\geq 0$.

Roots of unity $(\mu_m,\times)$ is a subgroup of $(\mu_n,\times)$ if $m|n$.

Properties of subgroups

Proposition 30

Let $(G,*)$ be a group and let $H\subseteq G$ be a nonempty subset. Then $(H,*)$ is a subgroup iff:

- (S1) For all $a,b\in H$, we have $a*b\in H$.
- (S2) For all $a\in H$, we have $a^{-1}\in H$.

Proposition 31

Let $(G,*)$ be a group and let $H\subseteq G$ be a nonempty subset. Then $(H,*)$ is a subgroup iff:

- (S) For all $a,b\in H$, we have $a*b^{-1}\in H$.

Proposition 32

Let $(G,*)$ be a group and let $H\subseteq G$ be a nonempty finite subset. Then $(H,*)$ is a subgroup iff

- (S1) For all $a,b\in H$, we have $a*b\in H$.

Intersection of subgroups

If $\{(H_i,*):i\in I\}$ is a collection of subgroups of $(G,*)$, then
$$\left(\bigcap_{i\in I}H_i,*\right)$$
is a non-empty subgroup of $(G,*)$.

Proposition 34

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

Symmetric groups

$(S_n,\circ)$

Let $X=\{1,2,\cdots,n\}$.
$$S_n=\{f:X\to X: f\text{ is a bijection}\}$$

- Let $\circ$ be the composition of functions. Then $(S_n,\circ)$ is the symmetric group (or permutation group on n letters).
- We can denote an element $k\in S_3$ by
$$k=\begin{pmatrix}1&2&3\\k(1)&k(2)&k(3)\end{pmatrix}$$
- The order of S_n is $n!$.

$(S_Y,\star)$

Let Y be an arbitrary set, not necessarily finite.
$$S_Y=\{f:Y\to Y: f\text{ is a bijection}\}$$
Let $\star$ be the composition of functions. Then $(S_Y,\star)$ forms a group.

- Let $Y=\{y_1,y_2,\cdots,y_n\}$ be a finite set of n elements. Then $(S_n,\circ)$ and $(S_Y,\star)$ are isomoprhic groups.

$(S_n'',\times)$

Let S_n'' be the set of all n by n permutation matrices (columns are a permutation of the standard basis vectors). Let $\times$ denote the usual matrix multiplication. Then $(S_n'',\times)$ forms a group.

- The groups $(S_n,\circ)$ and $(S_n'',\times)$ are isomorphic.

Cyclic notations

Fix $f\in S_n$. Let $x\in X=\{1,\cdots,n\}$. Consider the sequence of integers in X: $x_0,x_1,x_2,\cdots$, where $x_0=x$ and $x_i=f^i(x)\in X$.

- Since X is finite, the sequence will repeat. Let x_r be the first integer that repeats in the sequence. Can be shown that $x_r=x_0=x$.
- $\mathcal{O}=\{x_0,x_1,\cdots,x_{r-1}\}$ is an orbit of the powers of f.
- The sequence $(x_0x_1\cdots x_{r-1})$ is called a cycle.
- $X=\bigsqcup_j\mathcal{O}_j$

Example $f=(16)(24)(3789)(5)$

- f is also equal to $(61)(24)(8937)(5)$. We can rotate within the cycle.
- f is also equal to $(16)(24)(3789)$. We can drop singleton cycles.
- $h=(16)$ is the bijection in S_9 such that $h(1)=6,h(6)=1$ and $h(x)=x$ for $x\neq 1,6$.
- f is also equal to $(24)(16)(3789)(5)$. We can swap the cycles because they represent bijections in S_9 which are disjointed cycles and they are commutative.

Cyclic permutation A bijection $h \in S_n$ which is represented by a single cycle is called a cyclic permutation or cycle. Two cycles

$$h = (i_1 \cdots i_r) \text{ and } h' = (j_1 \cdots j_s)$$

are called disjointed cycles if $i_\alpha \neq j_\beta$ for all $\alpha = 1, \cdots, r$ and $\beta = 1, \cdots, s$.

Theorem 23 Let $f \in S_n$. Then

- $f = h_1 \circ h_2 \circ \cdots \circ h_r$ can be factorized into a product of mutually disjointed cycles.
- The factorization is unique up to an ordering of the product of cycles, i.e. if
$$f = h_1 \circ h_2 \circ \cdots \circ h_r = k_1 \circ k_2 \circ \cdots \circ k_s$$
are two factorization into mutually disjointed cycles, then by renaming the cycles k_i if necessary, we have $r = s$ and $h_i = k_i$ for $i = 1, \cdots, r$.

Transpositions A cycle $h \in S_n$ of the form $h = (ij)$ is a transposition.

- $(i_1 i_2 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_2)$. Hence, a cycle is a product of transpositions.
- Since $f \in S_n$ is a product of cycles, f is also a product of transpositions.

The sign character

Lemma For all permutation matrices $F, H \in S_n''$,

- $\det(F) = \det(F^T) = \pm 1$.
- $\det(FH) = \det(F)\det(H)$.

Proposition 25 Let $P(\boldsymbol{x}) = P(x_1, \cdots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)$. For $f \in S_n$, let

$$P_f(\boldsymbol{x}) = P_f(x_1, \cdots, x_n) = P(x_{f(1)}, \cdots, x_{f(n)}) = \prod_{1 \le i < j \le n} (x_{f(i)} - x_{f(j)})$$

- $P_f(\boldsymbol{x}) = P(\boldsymbol{x})$ or $-P(\boldsymbol{x})$. We write $P_f(\boldsymbol{x}) = \text{sgn}(f) P(\boldsymbol{x})$, where $\text{sgn}(f) = \pm 1$.
- $\text{sgn}(f \circ h) = \text{sgn}(f)\text{sgn}(h)$.

Even/odd Let $f, h \in S_n$.

- f is an even permutation if $\text{sgn}(f) = 1$, and odd if $\text{sgn}(f) = -1$.
- If f and h are both even (odd), then $f \circ h$ is even (odd).
- If f is odd and h is even, then $f \circ h$ is odd.
- A transposition is an odd permutation.
- A product of an even (odd) number of transpositions is even (odd).
- f is even $\iff$ f is a product of an even number of transpositions.

Alternating group Let

$$A_n = \{f \in S_n : \text{sgn}(f) = 1\} = \{f \in S_n : f \text{ even}\}$$

be the set of all even permutations in S_n. Then $(A_n, \circ)$ is a subgroup of $(S_n, \circ)$.

- The subset of odd permutations is not a subgroup.

Cayley's theorem

Let $(G, *)$ be a finite group of order n. Then $(G, *)$ is isomorphic to a subgroup of $(S_n, \circ)$.

Proof

- We know that $(S_Y, \circ)$ is isomorphic to $(S_n, \circ)$.
- Let $Y = G$. For every $g \in G$, define function $f_g : Y \to Y$ by
$$f_g(y) = g * y \text{ for all } Y = G$$
Then construct $\phi : G \to S_Y$ by $\phi(g) = f_g$. ϕ is an injective group homomorphism, so G is isomorphic to the image G' which is a subset of S_Y, i.e. G is isomorphic to a subgroup of $(S_Y, \circ)$.

Cosets and Lagrange's theorem

Coset

Let H be a subgroup of G. For $g \in G$, denote

$$gH = \{gh : h \in H\} \text{ and } Hg = \{hg : h \in H\}$$

These are called a left coset and a right coset of H in G respectively. Note that $eH = He = H$.

- If G is abelian, then a left coset is also a right coset.

Mutually disjointed subsets

Let S be a set, and let $\{S_i : i \in I\}$ be a collection of subsets of S.

- We say that $\{S_i : i \in I\}$ is a collection of mutually disjointed subsets if $S_i \cap S_j = \emptyset$ for every distinct $i, j \in I$.
- We say that $\{S_i : i \in I\}$ forms a partition of S if it is a collection of mutually disjointed subsets, and $S = \bigcup_{i \in I} S_i$. We write $S = \coprod_{i \in I} S_i$.

Proposition 37

Let G be a group and let H be a subgroup. Let $x, y, z \in G$.

i. If $z \in xH$, then $zH = xH$.
ii. If $xH \cap yH \neq \emptyset$, then $xH = yH$.
iii. The collection of left cosets $\{xH : x \in G\}$ forms a partition of G.
iv. Every coset xH is of the same cardinality as H, i.e. there is a bijection $f : H \to xH$. If H is a finite group, then $|H| = |xH|$.

Definition

- Denote $G/H = \{xH : x \in G\}$ and $H \backslash G = \{Hx : x \in G\}$.
- Let $[G : H]$ denote the number of distinct left cosets of H in G, i.e. $[G : H] = |G/H|$. It is called the index of H in G.

Lagrange's Theorem

Let G be a finite group and let H be a subgroup.

- $|H|$ divides $|G|$.
- $[G : H] = |G/H| = |G| / |H|$.
- $[H : G] = |H \backslash G| = |G| / |H|$.

Corollary Let p be a prime integer, and let G be a group of order p.

- The only subgroups of G are $\{e\}$ or G.
- Let $x \in G$ and $x \neq e$. Let $x = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ be the cyclic subgroup of G generated by x. Then $G = \langle x \rangle$.

Corollary If H is a subgroup of G and K is a subgroup of H, then

$$[G : K] = [G : H][H : K]$$

Generators

Subgroup Let G be a group, and let $X \subseteq G$. Let $S = \{H : H \text{ subgroup of } G, H \supseteq X\}$. We define

$$\langle X \rangle = \bigcap_{H \in S} H$$

and we call $\langle X \rangle$ the subgroup of G generated by X.

- If H is a subgroup of G containing X, then by definition, H contains $\langle X \rangle$. Hence, $\langle X \rangle$ is also called the smallest subgroup of G containing X.
- If the subgroup $\langle X \rangle = G$, then we say that G is generated by X.
- We say that a group G is finitely generated if it is generated by some finite subset. G could still be infinite, e.g. $G = (\mathbb{Z}, +)$ is generated by $X = \{1\}$.

Word A word on X is either e or a finite product $x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n} \in G$ where $x_i \in X$ and $r_i \in \mathbb{Z}$ for $i = 1, \cdots, n$.

- Some x_i can be the same.
- Some r_i may be negative integers.
- If G is non-abelian, order of multiplication matters.
- Two different words may represent the same element in G.

Proposition 39

Let X be a subset of a group G. Let W be the set of words on X. Then W is a subgroup and $W = \langle X \rangle$.

Cyclic groups

Proposition Let $(G, *)$ be a group. Pick $a \in G$. The subset $\langle a \rangle = \{a^n \in G : n \in \mathbb{Z}\}$ is a subgroup of $(G, *)$. It is called the cyclic subgroup of G generated by a.

- $\langle a \rangle = \langle a^{-1} \rangle$.

Proposition 40 The order of the subgroup $|\langle a \rangle|$ is equal to the order $o(a)$.

Proposition 41 Let G be a finite group. Let $a \in G$. Then $o(a)$ divides $|G|$.

Corollary 42 Let G be a finite group of order p where p is a prime number. Pick $a \in G$ and $a \neq e$. Then

$$G = \langle a \rangle = \{e, a, \cdots, a^{p-1}\}$$

Cyclic group

Let $(G, *)$ be a group and let $x \in G$. A group $(G, *)$ is called a cyclic gp if $G = \langle x \rangle$ for some $x \in G$, i.e.

$$G = \langle x \rangle = \{x^n \in G : n \in \mathbb{Z}\}$$

- Group G is cyclic $\implies$ some element $x \in G$ has order $|G|$

Group homomorphisms

Let $(G, *)$ and $(H, \star)$ be two groups. A function $\phi : G \to H$ is called a group homomorphism if

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

for all $x, y \in G$.

- There is no requirement on ϕ to be injective or surjective. But if ϕ is a bijection, then we have a group isomorphism instead.
- Composition of group homomorphisms is a group homomorphism.
- Let $\phi : (G, *) \to (H, \star)$ be an injective group homomorphism. Then $(G, *)$ is isomorphic to its image which is a subgroup of $(H, \star)$.

Proposition 43 Let $\phi : (G, *) \to (H, \star)$ be a group homomorphism.

i. Let e_G and e_H be identity elements of the groups G and H respectively. Then $\phi(e_G) = e_H$.
ii. For all $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$.
iii. Let G' be a subgroup of G. Then the image $\phi(G')$ is a subgroup of H.
iv. Let H' be a subgroup of H. Then $\phi^{-1}(H')$ is a subgroup of G.

Kernel Let $\phi : (G, *) \to (H, \star)$ be a group homomorphism. The kernel of ϕ is defined as

$$\ker \phi = \phi^{-1}(e_H) = \{g \in G : \phi(g) = e_H\}$$

It is the set of elements in G that is sent to e_H under the mapping ϕ.

Prop. 44 Let $\phi : (G, *) \to (H, \star)$ be a group homomorphism and let K be the kernel of ϕ.

i. The kernel K is a subgroup of G.
ii. $\forall g_0 \in K$ and $g \in G$, we have $g g_0 g^{-1} \in K$.
iii. For $g_0 \in G$, we have
$$\{g \in G : \phi(g) = \phi(g_0)\} = g_0 K = K g_0$$
i.e. every left coset of K is also a right coset.

Corollary 45 Let $\phi : (G, *) \to (H, \star)$ be a group homomorphism. Then ϕ is injective (as a function) $\iff$ $\ker \phi = \{e_G\}$.

Group homomorphisms and subgps

Let $(G, *)$ and $(H, \star)$ be two groups and let $\phi : (G, *) \to (H, \star)$ be a group homomorphism. Let $K = \ker \phi$. Define

- $\mathbf{Sub}(G, K) = \{G' : G' \text{ subgroup of } G, G' \supset K\}$ which contains all the subgroups of G which contain K and
- $\mathbf{Sub}(H) = \{H' : H' \text{ subgroup of } H\}$

Define a function $\Phi : \mathbf{Sub}(G, K) \to \mathbf{Sub}(H)$ by $\Phi(G') = \phi(G')$ where $G' \in \mathbf{Sub}(G, K)$. By proposition 43(iii), $\phi(G')$ is a subgroup of H, so $\Phi(G') \in \mathbf{Sub}(H)$.

Theorem 46 Suppose ϕ is a surjective homomorphism. Then Φ is a bijection.

Normal subgroups

Let G be a group and let N be a subgroup.

- N is called a normal subgroup of G if for all $n \in N$ and $g \in G$, $gng^{-1} \in N$.
- We denote a normal subgroup N of G by $N \lhd G$.
- Suppose G is abelian. Then every subgroup N of G is a normal subgroup.

Prop. 48 The kernel of a group homomorphism $\phi : (G, *) \to (H, \star)$ is a normal subgroup of G.

Center Let $(G, *)$ be a group. Let

$$Z = \{z \in G : zg = gz \text{ for all } g \in G\}$$

Z is a normal subgroup of G and it is called the center of G.

Proposition 49 Let K be a subgroup of G. The following statements are equivalent.

i. The subgroup K is normal, i.e. for all $k \in K$ and $g \in G$, $gkg^{-1} \in K$.

ii. For all $g \in G$, $gKg^{-1} = K$.

iii. For all $g \in G$, $gK = Kg$, i.e. every left coset is also a right coset.

iv. For all $g \in G$, $(gK)(g'K) = (gg')K$.

Notation If K is a subgroup of G and $gK = g'K$ for some $g, g' \in G$, we write

$$g \equiv g' \; (\text{mod}_L K)$$

The subscript L in mod_L denotes left cosets.

Simple groups

A group G is simple if its normal subgroups are only its trivial normal subgroups $\{e\}$ and G.

- Let p be a prime number. $\mathbb{Z}/p\mathbb{Z}$ is a simple group.

Theorem 50 Let

$$A_n = \{f \in S_n : \text{sgn}(f) = 1\} = \{f \in S_n : f \text{ even}\}$$

be the set of all even permutations in S_n.

- $(A_n, \circ)$ is a subgroup of $(S_n, \circ)$.
- For $n \neq 4$, the alternating group A_n is a simple group.

Lemma 51 Let H be a normal subgroup of A_n where $n \geq 5$. If H contains a 3-cycle, $H = A_n$.

- H contains a 3-cycle $\implies$ H contains all the 3-cycles of A_n. Every even permutation is the product of 3-cycles. Hence $H = A_n$.

Definition Let $X_n = \{1, 2, \cdots, n\}$. Recall that A_n is the set of even permutations on X_n. We can identify A_{n-1} as a subgroup of A_n by

$$A_{n-1} = \{\sigma \in A_n : \sigma(n) = n\}$$

Lemma 52 Let H be a normal subgroup of a group A. For subgroup A' of A, $H \cap A'$ is a normal subgroup of A'.

Quotient groups

Let $(G, *)$ be a group and let K be a normal subgroup. By proposition 49(iv), for all $g_1, g_2 \in G$, define the binary operation

$$(g_1 K) \diamond (g_2 K) = (g_1 g_2) K$$

for $g_1 K, g_2 K \in G/K$.

Theorem 56

i. The pair $(G/K, \diamond)$ forms a group. It is called the quotient group of G by K.

ii. The function $\pi : (G, \star) \to (G/K, \diamond)$ defined by $\pi(g) = gK$ for all $g \in G$ is a surjective group homomorphism. It is called the quotient map or quotient homomorphism.

iii. The kernel of π is K.

The First Isomorphism Theorem

In this section, $(G, *)$ and $(H, \star)$ are (possibly infinite) groups. Let $\phi : (G, *) \to (H, \star)$ be a surjective group homomorphism. Let K be the kernel of ϕ.

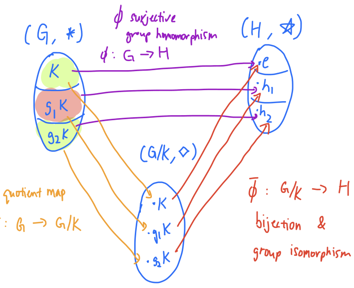
- Suppose $\phi(g) = h$ where $h \in H$ and $g \in G$. Then
$$\{x \in G : \phi(x) = h\} = gK$$
i.e. the whole of gK is sent to h under ϕ.

First Isomorphism Theorem

Let $\phi : (G, *) \to (H, \star)$ be a surjective group homomorphism. Let K be the kernel of ϕ. Then the function $\bar{\phi} : (G/K, \diamond) \to (H, \star)$ given by

$$\bar{\phi}(gK) = \phi(g)$$

is a well-defined group isomorphism.



- If ϕ is not surjective, then replace H with the image $H' = \phi(G)$ in the definition of $\bar{\phi}$.

Corollary Let $\phi : G \to H$ and $\psi : G \to H'$ be two group homomorphisms.

- Suppose ϕ and ψ have the same kernel K. Then, the images $\phi(G)$ and $\psi(G)$ are isomorphism groups.
- If G is a finite group, then
$$|\phi(G)| = |\psi(G)| = |G/K| = |G| \,/\, |K|$$

The Second Isomorphism Theorem

In this section, G is a group, M is a subgroup of G, and K is a normal subgroup of G.

Prop. 59 $MK = KM$ and it is a subgroup of G.

Proposition 60

i. The function $\phi : M \to MK/K$ defined by $\phi(m) = mK$ is a surjective group homomorphism.

ii. The kernel of ϕ is $M \cap K$. In particular, it is a normal subgroup of M.

Second Isomorphism Theorem

$$M/(M \cap K) \simeq (MK)/K$$

The Third Isomorphism Theorem

Let G be a group. Let M and K be normal subgroups of G such that $M \supseteq K$. Then M/K is a normal subgroup of G/K and

$$(G/K)/(M/K) \simeq G/M$$

If $M \not\supseteq K$, then replace K by $M \cap K$, which is a normal subgroup of G contained in M.

Corollary Let M and K be normal subgroups of G such that $M \supseteq K$. Then there is a surjective group homomorphism

$$\phi : G/K \to G/M$$

given by $\phi(gK) = gM$.

Euler's totient function

Let n be a positive integer. If $n = 1$, set $\Phi(1) = \{1\}$. Else set

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

- Let $*$ denote multiplication modulo n. Then $(\Phi(n), *)$ is a group.
- Let $\phi(n)$ denote the number of elements in $\Phi(n)$.
- For prime number p, $\Phi(p) = \{1, 2, \cdots p-1\}$, so $\phi(p) = p - 1$.
- For prime number p, let $n = p^r$.
$$\phi(p^r) = n - \frac{n}{p} = p^r\left(1 - \frac{1}{p}\right) = p^{r-1}(p-1)$$

Euler's theorem

Let x be an integer such that $\gcd(x, n) = 1$. Then

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

Calculating $\phi(n)$

Suppose $n = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) = \phi(p_1^{r_1})\phi(p_2^{r_2})\cdots\phi(p_k^{r_k})$$

Example Compute $43^{866} \pmod{360}$.

- $360 = 2^3 \cdot 3^2 \cdot 5$ so
$$\phi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 96$$
- Since $\gcd(43, 360) = 1$, Euler's theorem gives $43^{96} \equiv 1 \pmod{360}$.
- We have $866 = 96(9) + 2$ so
$$43^{866} \equiv 43^{96(9)+2} \equiv (43^{96})^9 43^2 \equiv 1^9 43^2 \equiv 49 \pmod{360}$$

Automorphism groups

Let $(G, *)$ be a group. An isomorphism $\phi : G \to G$ is called an automorphism of G. We denote the set of automorphisms of G by

$$\text{Aut}(G) = \{\phi : G \to G : \phi \text{ is an isomorphism}\}$$

Isomorphism facts

- Identity map id_G is an isomorphism.
- Composition of isomorphisms is an isomorphism, i.e. $\circ$ is a binary operation on $\text{Aut}(G)$.
- Inverse of an isomorphism is an isomorphism.

Proposition $(\text{Aut}(G), \circ)$ forms a group.

- It is called the automorphism group of G.
- A subgroup A of $(\text{Aut}(G), \circ)$ is called an automorphism subgroup.

Inner automorphism

Let G be a group and let $g \in G$. Then $\phi_g : G \to G$ given by

$$\phi_g(x) = gxg^{-1}$$

is a group automorphism. It is called an inner automorphism of G.

- Let $\text{Inn}(G) = \{\phi_g : g \in G\}$ be the set of inner automorphisms.
- The subset $\text{Inn}(G)$ is a normal subgroup of $(\text{Aut}(G), \circ)$.

Proposition The map $T : G \to \text{Inn}(G)$ given by $T(g) = \phi_g$ is a surjective group homomorphism whose kernel is the center of the group

$$Z(G) = \{z \in G : gz = zg \text{ for all } g \in G\}$$

By the first isomorphism theorem,

$$G/Z(G) \simeq \text{Inn}(G)$$

The Sylow Theorems

Notation Let n be a positive integer. Suppose p^e divides n, but p^{e+1} does not divide n. We write $p^e || n$. Alternatively, n $= p^e m$ where $p \not| \, m$.

Definition

Let G be a finite group of order n. Let p be a prime divisor of n. Let H be a subgroup of order of p^e.

- H is called a p-subgroup of G.
- If $p^e || n$, then H is called a Sylow p-subgroup of G.

Example Let $G = S_9$. It has order $9! = 2^7 3^4 5^1 7^1$.

- A subgroup of order 2^5 is a 2-subgroup.
- A subgroup of order 2^7 is a Sylow 2-subgroup.

First Sylow Theorem

Let G be a group of order n. Let p be a prime divisor of n. Then G contains a Sylow p-subgroup.

Corollary Let G be a finite group of order n. Let p be a prime divisor of n. If $p^d | n$, then G contains a subgroup of order p^d.

Definition

Let P be a subgroup of G. Let $g \in G$. Then gPg^{-1} is a subgroup of G called a conjugate of P. Let P be a Sylow p-subgroup. Then a conjugate gPg^{-1} is also a Sylow p-subgroup.

Theorem 94

Let G be a group of order n. Let $\{P_1, P_2, \cdots, P_r\}$ be all the distinct conjugates of a Sylow p-subgroup $P = P_1$.

i. Let Q be a p-subgroup of G. Then $Q \subseteq P_i$ for some i.

ii. (Second) If Q is a Sylow p-subgroup of G, then $Q = P_i$ for some i.

iii. (Third) Let r denote the number of Sylow p-subgroups of G. Then
$$r \equiv 1 \pmod{p} \text{ and } r | [G : P]$$

Corollary 95 Let P be a Sylow p-subgroup of a finite group G. Then P is a normal subgroup $\iff$ P is the unique Sylow p-subgroup of G.