Learning Group Theory
Rotman An introduction to the theory of groups

toshinari tong

February 13, 2023

1 Groups and homomorphisms

1.1 Permutations

If $X \neq \varnothing$, a **permutation** of X is a bijection $\alpha : X \to X$.

S_X denotes the set of all permutations of X.

S_n denotes the set of all permutations of $\{1, 2, ..., n\}$.

$|X|$ denotes the number of elements in a set $|X|$. ($|S_n| = n!$)

Define a function $\alpha : X \to X$ by $\alpha[i] = r_i$ for all $i \in X$. (r is a rearrangement of X)

It is an injection (i has no repetitions) and an surjection (all elements of X is in i)

New viewpoint: Any bijection α can be denoted by two rows:

$$\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha[1] & \alpha[2] & ... & \alpha[n] \end{pmatrix}$$

Composite of two bijections is again a bijection

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \alpha\beta \neq \beta\alpha$$

$\alpha \mid X$ means the function created by applying α on set X "alpha on X" ($X \subset$ domain of α)

EXERCISES

1. The identity function 1_X on a set X is a permutation, and we usually denote it by 1. Prove that $1\alpha = \alpha = \alpha 1$ for every permutation $\alpha \in S_X$.

$1(\alpha)[i] = 1[\alpha[i]] = \alpha[i] \quad \alpha(1)[i] = \alpha[1[i]] = \alpha[i]$

2. For each $\alpha \in S_X$, prove that there is $\beta \in S_X$ with $\alpha\beta = 1 = \beta\alpha$.

Let β be the inverse function of α. ($\beta(\alpha)[x] = x$ for all $x \in X$)

$\alpha(\beta)[\alpha[i]] = \alpha(\beta(\alpha))[i] = \alpha[\beta(\alpha)[i]] = \alpha[i] = 1[\alpha[i]] \quad \beta(\alpha)[j] = j = 1[j]$

3. For all $\alpha, \beta, \gamma \in S_X$, prove that $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

$p(q)[i] = p[q[i]]$

$\alpha(\beta(\gamma)))[i] = \alpha[\beta(\gamma)[i]] = \alpha[\beta[\gamma[i]]] \quad (\alpha(\beta))(\gamma)[i] = (\alpha(\beta))[\gamma[i]] = \alpha[\beta[\gamma[i]]] \quad$ for all $i \in X$

1.2 Cycles

If $x \in X$ and $\alpha \in S_X$, α **fixes** x if $\alpha[x] = x$ and α **moves** x if $\alpha[x] \neq x$.

Let $i_1, i_2, ..., i_r$ be distinct integers between 1 and n. If $\alpha \in S_n$ fixes the remaining $n-r$ integers and if

$$\alpha[i_1] = i_2, \alpha[i_2] = i_3, ..., \alpha[i_{r-1}] = i_r, \alpha[i_r] = i_1$$

then α is a r**-cycle**. Denote α by $(i_1\ i_2\ ...\ i_r)$.

A 2-cycle is called a **transposition**.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (1\ 5\ 3\ 4\ 2) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\ 2\ 3)(4)(5) = (1\ 2\ 3)$$

Multiplication with cycle notation:

$$\alpha = (1\ 2) \quad \beta = (1\ 3\ 4\ 2\ 5) \quad \gamma = \alpha\beta$$
$$\gamma(1) = \alpha(\beta(1)) = \alpha(3) = 3 \quad \gamma(3) = \alpha(\beta(3)) = \alpha(4) = 4 \quad \gamma(4) = 1 \quad \gamma(2) = 5$$
$$(1\ 2)(1\ 3\ 4\ 2\ 5) = (1\ 3\ 4)(2\ 5)$$

Two permutations $\alpha, \beta \in S_X$ are **disjoint** if every x moved by one is fixed by the other.

$\alpha[x] \neq x \implies \beta[x] = x$ and $\beta[x] \neq x \implies \alpha[x] = x$ (it is possible that $\alpha[x] = x = \beta[x]$).

A family of permutations $\alpha_1, \alpha_2, ..., \alpha_m$ is **disjoint** if each pair of them is disjoint.

EXERCISES (Note: all addition in indices assumed to loop around)

1. Prove that $(1\ 2\ ...\ r-1\ r) = (2\ 3\ ...\ r\ 1) = ... = (r\ 1\ ...\ r-2\ r-1)$.

   $\alpha_1[1] = 2, \alpha_1[2] = 3, ..., \alpha_1[r-1] = r \quad \alpha_2[2] = 3, \alpha_2[3] = 4, ..., \alpha_2[r] = 1 \quad ...$

   $\alpha_j[i] = i + 1 \quad (\alpha_j[r] = 1)$ for all $1 \leq j \leq n$

   There are r notations for all r-cycle.

2. If $1 \leq r \leq n$, then there are $n(n-1)...(n-r+1)/r$ r-cycles in S_n.

   Pick r distinct integers in different orders to form the r-cycles: $P_r^n = n(n-1)...(n-r+1)$

   Account for the r repetitions: $P_r^n/r = n(n-1)...(n-r+1)/r$

3. Prove that if $\alpha\beta = \alpha\gamma$ or $\beta\alpha = \gamma\alpha$, then $\beta = \gamma$.

   Consider an r-cycle of α, $(a_1\ a_2\ ...\ a_r)$

   Let $\beta[i]$ be a_j and $\gamma[i]$ be a_k: $\alpha[\beta[i]] = \alpha[a_j] = a_{j+1} \quad \alpha[\gamma[i]] = \alpha[a_k] = a_{k+1}$

   Since all elements in all r-cycles of α are distinct, $j = k$ and thus $\beta[i] = \gamma[i]$ for all i

   $\beta[\alpha[i]] = \gamma[\alpha[i]]$ If $\alpha : X \to Y$ and $\beta, \gamma : Y \to Z$ then $\beta = \gamma$

4. Let $\alpha = (a_1\ a_2\ ...\ a_r)$ and $\beta = (b_1\ b_2\ ...\ b_s)$. Prove that α and β are disjoint iff $\{a_1, a_2, ..., a_r\} \cap \{b_1, b_2, ..., b_s\} = \varnothing$.

   If $a \cap b = \varnothing$, $\alpha[a_i] \neq a_i$ and $a_i \notin b$ so $\beta[a_i] = a_i$ and vice versa $\therefore$ disjoint

   If $a \cap b \neq \varnothing$, there exists i, j such that $a_i = b_j$. $\alpha[a_i] \neq a_i$ and $\beta[b_j] \neq b_j$ $\therefore$ not disjoint

5. If α and β are disjoint permutations, then $\alpha\beta = \beta\alpha$; that is, α and β commute

If i is in an r-cycle of β $(b_1, b_2, ..., b_r)$ $(i = b_j)$, $\alpha[\beta[i]] = \alpha[\beta[b_j]] = \alpha[b_{j+1}]$

Since α and β are disjoint and b_{j+1} is moved by β, $\alpha[b_{j+1}] = b_{j+1}$

Similarly, $\beta[\alpha[i]] = \beta[\alpha[b_j]] = \beta[b_j] = b_{j+1}$ $\therefore \alpha[\beta[i]] = \beta[\alpha[i]] = b_{j+1}$

if i is fixed by β, $\alpha[\beta[i]] = \alpha[i]$ and $\beta[\alpha[i]] = \alpha[i]$

(If i is fixed by α, $\beta[\alpha[i]] = \beta[i] = i = \alpha[i]$;

else, $\beta[\alpha[i]] = \alpha[i]]$ since $\alpha[i]$ is part of a cycle of α, that is, it is moved by α)

6. If $\alpha, \beta \in S_n$ are disjoint and $\alpha\beta = 1$, then $\alpha = 1 = \beta$.

Let $(b_1, b_2, ..., b_r)$ be an r-cycle of β.

$\alpha[\beta[b_i]] = b_i$ and $\alpha[\beta[b_i]] = \alpha[b_{i+1}] = b_i$ for all $1 \leq i \leq r$

Since $b_{i+1} \neq b_i$, α moves all b_{i+1} and hence moves all b_i.

β moves b_i and α moves b_i; contradiction with disjoint

$\therefore \beta$ has no r-cycles so $\beta = 1$ so $\alpha = 1$

7. If $\alpha, \beta \in S_n$ are disjoint, prove that $(\alpha\beta)^k = \alpha^k\beta^k$ for all $k \geq 0$. Is this true if α and β are not disjoint?

If $x = a_i \in (a_1\ a_2\ ...\ a_r)$ (and $\beta[a_i] = a_i$ for all i since disjoint),

$(\alpha\beta)^k[x] = (\alpha\beta)^{k-1}(\alpha\beta)[a_i] = (\alpha\beta)^{k-1}(\alpha)[a_i] = (\alpha\beta)^{k-1}[a_{i+1}] =$

$(\alpha\beta)^{k-j}(\alpha\beta)[a_{i+j-1}] = (\alpha\beta)^{k-j}(\alpha)[a_{i+j-1}] = (\alpha\beta)^{k-j}[a_{i+j}] = ... = a_{i+k} = \alpha^k[x] = \alpha^k\beta^k[x]$

Similarly, if $x = b_i \in (b_1\ b_2\ ...\ b_r)$, $(\alpha\beta)^k[x] = b_{i+k} = \alpha^k[b_{i+k}] = \alpha^k\beta^k[x]$

Else, $(\alpha\beta)^k[x] = \alpha^k\beta^k[x] = x$

8. Show that a power of a cycle need not be a cycle.

Consider $\alpha = (a_1\ a_2\ ...\ a_r)$. $\alpha^r[a_i] = \alpha^{r-1}[a_{i+1}] = ... = a_{i+r} = a_i$ $\therefore \alpha^r = 1$

9. (i) Let $\alpha = (a_1\ a_2\ ...\ a_r)$ be an r-cycle. For every $j, k \geq 0$, prove that $\alpha^k[i_j] = i_{k+j}$ if subscripts are read modulo r.

$\alpha^k[i_j] = \alpha^{k-1}[i_{j+1}] = \alpha^{k-r+j}[i_r] = \alpha^{k-r}[i_{r+j}] = \alpha^{k-r}[i_j] = \alpha^{k-lr}[i_j] = i_{j+k-lr}$

where l is the largest integer such that $lr < k$ (ok dont ask me about if $j + k > r$)

(ii) Prove that if α is an r-cycle, then $\alpha^r = 1$, but that $\alpha^k \neq 1$ for every positive integer $k < r$.

$\alpha^k[a_i] = a_{i+k} \neq a_i$ $\therefore \alpha^k \neq 1$ (r proved at (8.))

(iii) If $\alpha = \beta_1\beta_2...\beta_m$ is a product of disjoint r-cycles β_i, then the smallest positive integer l with $\alpha^l = 1$ is the least common multiple of $\{r_1, r_2, ..., r_m\}$.

$\alpha^l = (\beta_1\beta_2...\beta_m)^l = \beta_1^l\beta_2^l...\beta_m^l$ (7.) $\therefore \beta_1^l = \beta_2^l = ... = \beta_m^l = 1$ (6.)

Since $\beta_i^k = 1$ when $r \mid k$, $r_i \mid l$ for all i. $\therefore$ smallest l is the lcm.

10. (i) A permutation $\alpha \in S_n$ is **regular** if either α has no fixed points and it is the product of disjoint cycles of the same length or $\alpha = 1$. Prove that α is regular iff α is a power of an n-cycle β; that is, $\alpha = \beta^m$ for some m.

If $\alpha = \beta^m = (b_1\ b_2\ ...\ b_n)^m$, $\alpha[b_i] = b_{i+m}$ (9.(i))

In α, b_i is in $(b_i\ b_{i+m}\ b_{i+2m}\ ...)$, which is of length k.

Since all b_i are in cycles of length k, α is regular.

If $\alpha = (a_1\ a_2\ ...\ a_k)(b_1\ b_2\ ...\ b_k)...(z_1\ z_2\ ...\ z_k)$ is regular, let $\beta = (a_1\ b_1\ ...\ z_1\ a_2\ b_2\ ...\ z_2\ ...\ z_k)$

$\beta^m = \alpha$ since $\beta^m[x_i] = x_{i+m}$ (9.(i))

(ii) If α is an n-cycle, then α^k is a product of $gcd(n,k)$ disjoint cycles, each of length $n/gcd(n,k)$.

$\alpha^k = (a_1\ a_2\ ...\ a_n)^k$ (assume $k < n$ as $\alpha^n = 1$), $\alpha^k[a_i] = a_{i+k}$ (9.(i))

In α^k, a_i is in $(a_i\ a_{i+k}\ a_{i+2k}\ ...)$, which is of length l, then l is the smallest integer s.t. $n \mid lk$.

$l \mid n$ as all the cycles are of same length; Let $l = n/q$. Then, $n \mid lk$ $\ n \mid (nk/q)$ $\ \therefore q \mid k$

For l to be smallest, $q = gcd(n,k)$ as $q \mid n, k$. $\therefore l = n/gcd(n,k)$

(iii) If p is a prime, then every power of a p-cycle is either a p-cycle or 1.

π^k is a product of $gcd(p,k)$ disjoint cycles. (9.(ii))

$gcd(p,k) = p$ ($\pi^p = 1$) when $k = p$ and $gcd(p,k) = 1$ (π^k is a p-cycle) otherwise.

11. (i) Let $\alpha = \beta\gamma$ in S_n, where β and γ are disjoint. If β moves i, then $\alpha^k[i] = \beta^k[i]$ for all $k \geq 0$.

Since β moves i and all elements in its cycle, γ fixes all elements in that cycle.

$\therefore \alpha^k[i] = (\beta\gamma)^k[i] = \beta^k[i]$

(ii) Let α and β be cycles in S_n. If there is i_1 moved by both α and β and if $\alpha^k[i_1] = \beta^k[i_1]$ for all positive integers k, then $\alpha = \beta$.

Let α, β be $(a_1\ a_2\ ,,,\ a_n)$ and $(b_1\ b_2\ ,,,\ b_m)$ where $a_1 = b_1 = i_1$. WLOG assume $n \leq m$

Since $\alpha^k[i_1] = \beta^k[i_1]$, $a_2 = b_2, a_3 = b_3, ..., a_n = b_n$. $\alpha[a_n] = \beta[b_n]$ so $a_1 = b_{n+1} = b_1$

However all elements of b is distinct, so $n = m$ $\therefore \alpha = \beta$

1.3 Factorization into Disjoint Cycles

Let us factor $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}$ into a product of disjoint cycles.

Starting from 1, $\alpha[1] = 6, \alpha[6] = 3, \alpha[3] = 1$ so (1 6 3); Smallest integer not having

appeared is 2, which becomes (2 4). Continuing like this, $\alpha = (1\ 6\ 3)(2\ 4)(5)(7\ 8\ 9)$

Theorem 1.1 *Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.*

Proof. The proof is by induction on the number k of points moved by α.

Base case $k = 0$ is true, for then $\alpha = 1$.

If $k > 0$, let i_1 be a point moved by α. Define $i_j = \alpha[i_{j-1}]$ for all $j > 1$.

Define r as the smallest integer for which $i_{r+1} \in \{i_1, i_2, ..., i_r\}$.

We claim that $\alpha[i_r] = i_1$. Otherwise, $\alpha[i_r] = i_j$ for some $j > 1$,

but $\alpha[i_{j-1}] = i_j$, contradicting α is an injection.

Let X be the set of points $\{i_1, i_2, ..., i_r\}$ and σ be the r-cycle $(i_1\ i_2\ ...\ i_r)$. If $r = n$, $\alpha = \sigma$.

If $r < n$ and Y is the set of remaining $n - r$ points, then $\alpha[Y] = Y$ and σ fixes points in Y.

$\sigma \mid X = \alpha \mid X$ ($\alpha \mid X$ means the function on domain X "alpha on X")

If α' is the permutation with $\alpha' \mid Y = \alpha \mid Y$ and which fixes X,

then σ and α' are disjoint and $\alpha = \sigma\alpha'$.

Since α' moves fewer point than α, α', and hence α, is a product of disjoint cycles by induction.

A **complete factorization** of a permutation α is a factorization which contains one 1-cycle (i) for every i fixed by α.

Theorem 1.2 *Let $\alpha \in S_n$ and alpha $= \beta_1\beta_2...\beta_t$ be a complete factorization. This factorization is unique except for the order in which the factors occur.*

Proof. Disjoint cycles commute (1.2.5) so the order of factors is not uniquely determined.

Suppose $\alpha = \gamma_1\gamma_2...\gamma_s$ is a second complete factorization into disjoint cycles.

If β_t moves i_1, some γ_j moves i_1, and we may assume that $\gamma_j = \gamma_s$ as disjoint cycles commute.

$\beta_t^k[i_1] = \gamma_s^k[i_1] = \alpha^k[i_1]$ (1.2.11(i)) $\therefore \beta_t = \gamma_s$ (1.2.11(ii))

The cancellation law (1.2.3) gives $\beta_1\beta_2...\beta_{t-1} = \gamma_1\gamma_2...\gamma_{s-1}$.

By induction on $max(s, t)$, the factorization is unique.

EXERCISES

1. Let α be the permutation of $\{1, 2, ..., 9\}$ defined by $\alpha[i] = 10 - i$. Factorize α.

$\alpha = (1\ 9)(2\ 8)(3\ 7)(4\ 6)(5)$

2. Let p be a prime and let $\alpha \in S_n$. If $\alpha^p = 1$, then either $\alpha = 1$, α is a p-cycle, or α is a product of disjoint p-cycles.

Let $\alpha = \beta_1\beta_2...\beta_t$ be the complete factorization of α.

$\alpha^p = (\beta_1\beta_2...\beta_t)^p = \beta_1^p\beta_2^p...\beta_t^p = 1$ (1.2.7) and $\beta_1^p, \beta_2^p, ..., \beta_t^p$ are disjoint (1.2.9(i))

$\therefore \beta_1^p = \beta_2^p = ... = \beta_t^p = 1$ (1.2.6)

β_i^p is a product of $gcd(r_i, p)$ disjoint cycles where r_i is length of β_i (1.2.10(ii))

Since $\beta_i^p = 1$, $gcd(r_i, p) = r_i$, which is only possible if $r_i = k_i p$

The smallest integer l where $\alpha^l = 1$ is the lcm of $\{r_1, r_2, ..., r_t\} = \{k_1 p, k_2 p, ..., k_t p\}$ (1.2.9(iii))

However, $l = p$ since all m which satisfies $\alpha^m = 1$ must be a multiple of l, and p is a prime.

$\therefore lcm(k_1 p, k_2 p, ..., k_t p) = p$ so all $k_i = 1$ and all β_i are p-cycles. (Of course, if $\alpha = 1$, $\alpha^p = 1$)

3. How many $\alpha \in S_n$ are there with $\alpha^2 = 1$?

From (2), $\alpha = 1$ or $\alpha = \beta_1 \beta_2 ... \beta_t$ where β_i are all disjoint 2-cycles.

$$x = \sum_{i=0}^{2i \leq n} \binom{n}{2i} \frac{(2i)!}{2^i i!} = \sum_{i=0}^{2i \leq n} \binom{n}{2i} (2i-1)!!$$

(A000085 number of self-inverse permutations)

4. Give an example of permutations α, β, γ in S_5 with α commuting with β, β commuting with γ, but with α not commuting with γ.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

1.4 Even and Odd Permutations

A **transposition** is a 2-cycle.

Theorem 1.3 *Every permutation $\alpha \in S_n$ is a product of transpositions.*

Proof. By Theorem 1.1, it suffices to factor cycles:

$$(i_1\ i_2\ ...\ i_r) = (i_1\ i_r)(i_1\ i_{r-1})...(i_1\ i_2) \qquad \text{note that } i_j : j \mapsto 1 \mapsto (j+1)$$

Such factorization is not as nice as complete factorization: the transpositions need not commute, and neither the factors nor the number of factors are uniquely determined.

However, the parity of the number of factors is the same for all factorizations.

A permutation $\alpha \in S$ is **even** if it is a product of an even number of transpositions; otherwise α is **odd**.

However, the above definition doesn't account for if α has factorizations of both even and odd number of transpositions.

Lemma 1.4 *If $k, l \geq 0$, then*
$(a\ b)(a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l) = (a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l)$ *and*
$(a\ b)(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l) = (a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l)$

Proof. Directly evaluating, (letting L.H.S. be $f \cdot g = f(g(x))$)

$$f(g(a)) = f(c_1) = c_1 \qquad f(g(b)) = f(d_1) = d_1$$

$$f(g(c_i)) = f(c_{i+1}) = c_{i+1} \qquad f(g(d_i)) = f(d_{i+1}) = d_{i+1}$$

$$f(g(c_k)) = f(b) = a \qquad f(g(d_l)) = f(a) = b$$

$\therefore (a\ b)(a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l) = (a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l)$

$(a\ b)(a\ b)(a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l) = (a\ b)(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l)$

$\therefore (a\ b)(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l) = (a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l)$

If $\alpha \in S_n$ and $\alpha = \beta_1 ... \beta_t$ is a complete factorization into disjoint cycles, **signum** α is defined by

$$sgn(\alpha) = (-1)^{n-t}$$

By Theorem 1.2, t is unique for all α so sgn is a well-defined function.

If τ is a transposition, $t = (n-2) + 1 = n - 1$ ($(n-2)$ 1-cycles and 1 swap), so

$$sgn(\tau) = (-1)^{n-(n-1)} = -1$$

Lemma 1.5 *If $\beta \in S_n$ and τ is a transposition, then $sgn(\tau\beta) = -sgn(\beta)$*

Proof. Let $\tau = (a\ b)$ and $\beta = \gamma_1 ... \gamma_t$ be a complete factorization of β into disjoint cycles.

If a and b occur in the same γ_i, by Lemma 1.4,

$$\tau\gamma_i = (a\ b)(a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l) = (a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l) \qquad k, l \geq 0$$

On the other hand, if a and b occur in different γ_i and γ_j, by Lemma 1.4,

$$\tau\gamma_i\gamma_j = (a\ b)(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l) = (a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l) \qquad k, l \geq 0$$

$\therefore \tau\beta$ either consists of 1 more or 1 fewer cycle than β, so $sgn(\tau\beta) = -sgn(\beta)$.

Theorem 1.6 *For all $\alpha, \beta \in S_n, sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$.*

Proof. Assume $\alpha = \tau_1 ... \tau_m$ is a factorization of α into transpositions with minimal m.

The factorization $\tau_1 ... \tau_{m-1}$ is also minimal:

If there is one with less transpositions ($\sigma_1 ... \sigma_q = \tau_1 ... \tau_{m-1}$),

then $\alpha = \tau_1 ... \tau_m$ would not be minimal ($\sigma_1 ... \sigma_q \tau_m$ would be better).

$\therefore$ For all $1 \leq k \leq m$ factorization $\tau_1 ... \tau_k$ is minimal.

We prove by induction on m that $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$ for every $\beta \in S_n$.

The base case $m = 1$ is Lemma 1.5: $sgn(\tau_1\beta) = -sgn(\beta) = sgn(\tau_1)sgn(\beta)$

If $m > 1$, assuming $sgn(\tau_1 ... \tau_{m-1}\beta) = sgn(\tau_1 ... \tau_{m-1})sgn(\beta)$,

$$\begin{aligned}
sgn(\alpha\beta) &= sgn(\tau_1 ... \tau_m\beta) \\
&= -sgn(\tau_1 ... \tau_{m-1}\beta) && \text{(Lemma 1.5)} \\
&= -sgn(\tau_1 ... \tau_{m-1})sgn(\beta) && \text{(by induction)} \\
&= sgn(\tau_1 ... \tau_m)sgn(\beta) && \text{(Lemma 1.5)} \\
&= sgn(\alpha)sgn(\beta)
\end{aligned}$$

Theorem 1.7 *A permutation $\alpha \in S_n$ is even iff $sgn(\alpha) = 1$;*
A permutation $\alpha \in S_n$ is odd iff it is a product of an odd number of transpositions.

Proof. If $\alpha = \tau_1 ... \tau_m$, by Theorem 1.6, $sgn(\alpha) = sgn(\tau_1) ... sgn(\tau_m) = (-1)^m$.

If $sgn(\alpha) = 1$, then m is even, so α is even. Conversely, if α is even,

there exist a factorization into transpositions with m even, so $sgn(\alpha) = 1$ (sgn is well-defined).

If m is odd, $sgn(\alpha) = (-1)^m = -1$; since α is even iff $sgn(\alpha) = 1$, α must be odd.

Conversely, if α is odd, it has no factorizations into an even number of transpositions (or it will be even), so m must be odd.

EXERCISES

1. Show that an r-cycle is an even permutation iff r is odd.

$$(i_1\ i_2\ ...\ i_r) = (i_1\ i_r)(i_1\ i_{r-1})...(i_1\ i_2)$$

If r is odd, the above factorization consists of $r-1$, hence even number of transpositions.

By definition, the r-cycle is even. Conversely, if it is even, $sgn(\alpha) = 1$ from Theorem 1.7.

$\therefore (-1)^{n-t} = 1$, where t is the number of disjoint cycles in the complete factorization of α.

But α is just an r-cycle, so $t = 1$.

$\therefore n-1$ is even, thus n, hence r is odd. (only an n-cycle $\in S_n$, so $n = r$).

2. Compute $sgn(\alpha)$ for $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$.

Factorizing, $\alpha = (1\ 9)(2\ 8)(3\ 7)(4\ 6)(5)$; $sgn(\alpha) = (-1)^{9-5} = 1$.

Also, $\alpha = (1\ 9)(2\ 8)(3\ 7)(4\ 6)(5\ 1)(1\ 5)$

3. Show that S_n has the same number of even permutations as of odd permutations.

Consider function $f : S_n \to S_n$ where $f(\alpha) = (1\ 2)\alpha$.

(Assume $n > 1$; if $n = 1$, there is only 1 even permutation because $sgn(\alpha) = (-1)^{1-1} = 1$)

If α is even, $f(\alpha)$ is odd, vice versa. If there were x and y even and odd permutations in S_n, there would be x and y even and odd permutations in $f(S_n)$.

However, $f(S_n) = S_n$, so $x = y$.

4. Let $\alpha, \beta \in S_n$. If α and β have the same parity, then $\alpha\beta$ is even; if α and β have distinct parity, then $\alpha\beta$ is odd.

By Theorem 1.7, α is even iff $sgn(\alpha) = 1$; therefore α is odd (and not even) iff $sgn(\alpha) = -1$.

If α and β are both even or both odd, $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta) = 1$, so $\alpha\beta$ is even.

If α and β have distinct parity, $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta) = -1$, so $\alpha\beta$ is odd.

1.5 Semigroups

A binary **operation** on a nonempty set G is a function $\mu : G \times G \to G$.

The **Law of Substitution** states that $(a = a' \text{ and } b = b') \implies a * b = a' * b'$;
(just another way of saying μ is well-defined)

An operation $*$ on a set G is **associative** if $(a * b) * c = a * (b * c)$ for every $a, b, c \in G$.

Theorem 1.8 *If $*$ is an associative operation, every expression $a_1 * a_2 * ... * a_n$ needs no parentheses.*

Proof. The proof is by induction on $n \geq 3$. The base case $n = 3$ obviously holds.

Assume case $n = l$ holds for all $l \leq k$. Consider the last operation used is between a_i and a_{i+1};

then the expression can be expanded to $(a_1 * ... * a_i) * (a_{i+1} * ... * a_k)$

Compare 2 choices $(a_1 * ... * a_i) * (a_{i+1} * ... * a_k)$ and $(a_1 * ... * a_j) * (a_{j+1} * ... * a_k)$: (wlog $i \leq j$)

If $i = j$, the 2 products are equal; if $i < j$, rewrite the expressions to:

$(a_1 * ... * a_i) * ((a_{i+1} * ... * a_j) * (a_{j+1} * ... * a_k))$ $\quad$ $((a_1 * ... * a_i) * (a_{i+1} * ... * a_j)) * (a_{j+1} * ... * a_k)$

By induction, each of the 3 small expressions yield uniquely defined elements, and by associativity the 2 products are the same.

A **semigroup** $(G, *)$ is a nonempty set G equipped with an associative operation $*$.

Let G be a semigroup and $a \in G$. Define $a^1 = a$ and $a^{n+1} = a * a^n$ $(n \geq 1)$

Corollary 1.9 *Let m, n be positive integers. $a^m * a^n = a^{m+n} = a^n * a^m$ and $(a^m)^n = a^{mn} = (a^n)^m$*

Proof. Both sides of the first or second equations arise from an expression with $m + n$ or mn factors equal to a. By Theorem 1.8, they don't need parentheses.

When the operation is denoted by $+$, a^n is denoted as na;

Corollary 1.9 becomes $ma + na = (m + n)a = na + ma$ and $n(ma) = (mn)a = m(na)$

1.6 Groups

A **group** is a semigroup G containing an element e such that:

1. $e * a = a = a * e$ for all $a \in G$
2. for every $a \in G$, there is an element $b \in G$ with $a * b = e = b * a$

From exercises (1.1.1), (1.1.2), (1.1.3) , S_X is a group with composition as operation;

S_X is called the **symmetric group** on X.

When $X = \{1, 2, ..., n\}$, S_X is denoted S_n and called the **symmetric group on n letters**.

A pair of elements a and b in a semigroup **commutes** if $a * b = b * a$.

A group or a semigroup is **abelian** if every pair of its elements commutes.

Examples of groups:

1. $\mathbb{Z}$ is an abelian group with addition as operation $(e = 0, -a + a = 0)$;

   $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are also additive abelian group (a semigroup with 1 under multiplication)

2. Define congruence class $[a]$ of an integer a mod n by $[a] = \{a + kn : k \in \mathbb{Z}\}$

   set $\mathbb{Z}_n$ of all congruence classes mod n is an abelian group under operation $[a] + [b] = [a + b]$

   ($\mathbb{Z}_n$ is a commutative ring with $[1]$ under operation $[a][b] = [ab]$)

3. If k is a field, set of all $n \times n$ invertible matrices with entries in k is a group $\mathrm{GL}(n, k)$

   The operation of general linear group is matrix multiplication with e being the identity matrix

   $\mathrm{GL}(n, k)$ is only abelian when $n = 1$, which is the multiplicative group $k^\times$ of nonzero element in k

4. If R is an associative ring, u is a unit in R if there exists $v \in R$ with $uv = 1 = vu$

   If a is a unit, ua is also a unit so $U(R)$, the group of units in R, is a multiplicative group

   If k is a field, $U(k) = k^\times$ and $U(M_n(k)) = \mathrm{GL}(n, k)$

Theorem 1.10 *If G is a group, $\exists! e\, \forall a \in G\ (e * a = a = a * e)$ and $\forall a \in G\ \exists! b\ (a * b = e = b * a)$*

Proof. Suppose there is another e' s.t. $\forall a \in G(e' * a = a = a * e')$. If $a = e$, $e' * e = e$.

However, the defining property of e gives $e' * e = e'$, so $e' = e$.

Suppose that $a * c = e = c * a$. Then $c = c * e = c * (a * b) = (c * a) * b = e * b = b$.

With the uniqueness assertions, we can call e the **identity** of G and b (or a^{-1}) the **inverse** of a.

Corollary 1.11 *If G is a group and $a \in G$, $(a^{-1})^{-1} = a$.*

Proof. By definition, $a^{-1} * (a^{-1})^{-1} = e$. But $a^{-1} * a$ is also equal to e, so by uniqueness $(a^{-1})^{-1} = a$.

If G is a group and $a \in G$, the **powers** of a are as follows: $a^0 = e$; If $n \in \mathbb{Z}^+$, a^n is defined as in any semigroup and a^{-n} is defined as $(a^{-1})^n$.

Theorem 1.12 *If G is a semigroup with $e \in G$ s.t. $\forall a \in G\ (e * a = a)$ and $\forall a \in G\ \exists b \in G\ (b * a = e)$, then G is a group.*

Proof. If $x * x = x$, then $x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e$.

If $b * a = e$, then $(a * b) * (a * b) = a * (b * a) * b = a * e * b = a * b$. From above, $a * b = e$.

$a = a * e = a * (a^{-1} * a) = (a * a^{-1}) * a = e * a$

The above theorem simplifies the process of proving a particular example is a group.

EXERCISES

1. If G is a group and $a_1, a_2, ..., a_n \in G$, then $(a_1 * a_2 * ... * a_n)^{-1} = a_1^{-1} * a_2^{-1} * ... * a_n^{-1}$.

   $e = (a_1 * a_1^{-1}) * (a_2 * a_2^{-1}) * ... * (a_n * a_n^{-1}) = (a_1 * a_2 * ... * a_n) * (a_1^{-1} * a_2^{-1} * ... * a_n^{-1})$

   If $n \geq 0$, then $(a^n)^{-1} = (a^{-1})^n$.

2. Let $a_1, a_2, ..., a_n$ be elements of an abelian semigroup. If $b_1, b_2, ...b_n$ is a rearrangement of a, then $a_1 * a_2 * ... * a_n = b_1 * b_2 * ... * b_n$.

   Prove by induction on n: let $1 \leq k \leq n$ s.t. $b_k = a_n$.

   Since abelian, $(b_1 * ... * b_k) * (b_{k+1} * ... * b_n) = (b_{k+1} * ... * b_n) * (b_1 * ... * b_k)$

   $n = 1$ obviously holds, and proved by rearranging the first $n - 1$ terms in the same way

3. Let a and b lie in semigroup G. If a and b commute, then $(a * b)^n = a^n * b^n$ for every $n \geq 1$; if G is a group, then the equation holds for every $n \in \mathbb{Z}$.

   Proof by induction: $(a*b)^n = a*(b*a)^{n-1}*b = a*(a*b)^{n-1}*b = a*(a^{n-1}*b^{n-1})*b = a^n*b^n$

   $(b * a)^{-1} * b * a = e \implies a^{-1} = (b * a)^{-1} * b \qquad b * a * (b * a)^{-1} = e \implies b^{-1} = a * (b * a)^{-1}$

   $a^{-1} * b^{-1} = (b * a)^{-1} * b * a * (b * a)^{-1} = (b * a)^{-1} = (a * b)^{-1}$ (a and b commute)

$(a*b)^{-n} = ((a*b)^{-1})^n = (a^{-1}*b^{-1})^n = (a^{-1})^n * (b^{-1})^n = a^{-n}*b^{-n}$

4. A group in which $x^2 = e$ for every x must be abelian.

$a*b = a*(a*b)^2*b = a*a*b*a*b*b = a^2*b*a*b^2 = b*a$

5. (i) Let G be a finite abelian group containing no elements $a \neq e$ with $a^2 = e$. Evaluate $a_1 * a_2 * ... * a_n$, where $a_1, a_2, ..., a_n$ is a list with no repetitions, of all the elements in G.

Exclude e from the list. Let $1 \leq j \leq n$ s.t. $a_j = (a_i)^{-1}$. Since $(a_i)^2 \neq e$, $i \neq j$.

Therefore the list can be rearranged to pairs (abelian) and the result is e.

(ii) Prove **Wilson's theorem**: If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$

$\forall x \in \mathbb{Z}_p \backslash 0$, $1 \times x \equiv x \pmod{p}$.

Let $a, b \in \mathbb{Z}_p \backslash 0$ s.t. $a \neq b$. If $ax \equiv bx \pmod{p}$, $(a-b)x \equiv 0 \pmod{p}$.

But $a - b \neq 0$ and $x \neq 0$, so $ax \not\equiv bx \pmod{p}$.

Since $ax \pmod{p}$ is distinct for all a, There must exist $ax \equiv 1 \pmod{p}$.

Therefore $\mathbb{Z}_p \backslash 0$ is a group under modular multiplication. (Theorem 1.12)

If $x^2 = 1 \pmod{p}$, $(x+1)(x-1) \equiv 0 \pmod{p}$ so $x = 1$ or $x = p-1$.

$2, 3, ..., p-2$ can be arranged into pairs of (a, a^{-1});

Therefore $2 \times 3 \times ... \times (p-2) \equiv 1 \pmod{p}$ and $(p-1)! \equiv p-1 \pmod{p}$.

6. (i) If $\alpha = (1\ \ 2\ \ ...\ \ r-1\ \ r)$, then $\alpha^{-1} = (r\ \ r-1\ \ ...\ \ 2\ \ 1)$.

$\alpha^{-1}[\alpha[i]] = \alpha^{-1}[i+1] = i+1-1 = i$ so $\alpha^{-1}\alpha = e$. $(\alpha^{-1}[\alpha[r]] = \alpha^{-1}[1] = r)$

(ii) Find the inverse of $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

7. Show that $\alpha : \mathbb{Z}_{11} \to \mathbb{Z}_{11}$, defined by $\alpha(x) = 4x^2 - 3x^7$, is a permutation of $\mathbb{Z}_{11}$ and write it as a product of disjoint cycles. What is the parity of α and what is α^{-1}

From computation, $\alpha = (0)(1)(2\ \ 6\ \ 10\ \ 7)(3\ \ 9\ \ 4\ \ 5)(8)$ so $sgn(\alpha) = (-1)^{11-5} = -1$

$\alpha^{-1} = (0)(1)(7\ \ 10\ \ 6\ \ 2)(5\ \ 4\ \ 9\ \ 3)(8)$

8. Let G be a group, $a \in G$, and $m, n \in \mathbb{Z}$. Prove that $a^m * a^n = a^{m+n} = a^n * a^m$ and $(a^m)^n = a^{mn} = (a^n)^m$

If 1 of them is negative (WLOG $-m < 0$), $a^{-m} * a^n = (a^{-1})^m * a^m * a^{n-m} = a^{n-m}$

$(a^{-m})^n = ((a^{-1})^m)^n = (a^{-1})^{mn} = a^{-mn}$ $(a^n)^{-m} = ((a^n)^{-1})^m = ((a^{-1})^n)^m$ (1.6.1) $= a^{-mn}$

If both are negative, $a^{-m} * a^{-n} = (a^{-1})^{-m} * (a^{-1})^{-n} = (a^{-1})^{m+n} = a^{-m-n}$

$(a^{-m})^{-n} = (((a^{-1})^m)^{-1})^n = (((a^{-1})^{-1})^m)^n$ (1.6.1) $= a^{mn}$

9. In a group G, either of the equations $a*b = a*c$ and $b*a = c*a$ implies $b = c$.

$a * b = a * c \implies a^{-1} * a * b = a^{-1} * a * c \implies b = c$ similarly $b * a = c * a \implies b = c$

10. (i) For each $a \in G$, prove that the functions $L_a : G \to G$, defined by $x \mapsto a * x$ (**left translation** by a) and $R_{a:G \to G}$, defined by $x \mapsto x * a^{-1}$ (**right translation** by a) are bijections.

If $L_a(x) = L_a(y)$, $a * x = a * y$ and from (1.6.9) $x = y$.

$\therefore$ there are n distinct outputs and codomain G only has n elements, so it is a bijection.

Similarly, R_a is also a bijection.

(ii) For all $a, b \in G$, prove that $L_{a*b} = L_a \circ L_b$ and $R_{a*b} = R_a \circ R_b$.

$L_a(L_b(x)) = a * b * x = L_{a*b}(x)$

$R_a(R_b(x)) = x * b^{-1} * a^{-1} = x * (a * b)^{-1}$ (1.6.3) $= R_{a*b}(x)$

(iii) For all a and b, prove that $L_a \circ R_b = R_b \circ L_a$.

$L_a(R_b(x)) = a * (x * b^{-1}) = (a * x) * b^{-1} = R_b(L_a(x))$

11. Let G denote the multiplicative group of positive rationals. What is the identity of G? If $a \in G$, what is its inverse?

$(\forall r \in \mathbb{R}) \quad 1 \times r = r = r \times 1 \quad a \times \frac{1}{a} = 1 = \frac{1}{a} \times a$

12. Let n be a positive integer and let G be the multiplicative group of all nth roots of unity. What is the identity of G? If $a \in G$, what is its inverse? How many elements does G have?

$(\forall k \in \mathbb{Z}) \quad 1 \times e^{2\pi ik/n} = e^{2\pi ik/n} = e^{2\pi ik/n} \times 1 \quad e^{2\pi ik/n} * e^{-2\pi ik/n} = 1 = e^{2\pi ik/n} * e^{-2\pi ik/n}$

Since $e^{2\pi in/n} = 1$, $e^{2\pi ik/n} = e^{2\pi i(k+an}/n$ where $a \in \mathbb{Z}$. So there are n elements in G.

13. Prove that the following four permutations form a group $\mathbb{V}$: (called the **4-group**) $(1)(2)(3)(4)$, $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$

$(\forall \alpha \in \mathbb{V})$ $((1)(2)(3)(4))\alpha = \alpha = \alpha((1)(2)(3)(4))$ and $\alpha^2 = (1)(2)(3)(4) \implies \alpha = \alpha^{-1}$

14. Let $\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ and define $1/0 = \infty, 1/\infty = 0, \infty/\infty = 1, 1 - \infty = \infty = \infty - 1$. Show that the 6 functions $\hat{\mathbb{R}} \to \hat{\mathbb{R}}$ given by $x, 1/x, 1 - x, 1/(1 - x), x/(x - 1), (x - 1)/x$ form a group with composition as operation.

Call the 6 functions $f_1, ..., f_6$. Computing, $(f_1(0), ..., f_6(0)) = (0, \infty, 1, 1, 0, -\infty)$,

$(f_1(1), ..., f_6(1)) = (1, 1, 0, \infty, \infty, 0)$, $(f_1(\infty), ..., f_6(\infty)) = (\infty, 0, \infty, 0, 1, 1)$

$-(1 - \infty) = \infty - 1 \implies -\infty = \infty$ so $f_6(0) = \infty$. Also, $(\forall a \in \mathbb{R}\backslash\{0, 1\})$ $f_i(a) \in \mathbb{R}$

Moreover, $f_2(f_2(a)) = f_3(f_3(a)) = f_5(f_5(a)) = f_4(f_6(a)) = f_6(f_4(a)) = a$,

f_1 is obviously e. From above, $f_2 \circ f_2 = f_3 \circ f_3 = f_5 \circ f_5 = f_4 \circ f_6 = f_6 \circ f_4 = e$.

Therefore, all elements have inverses and thus the functions form a group.

1.7 Homomorphisms

Let G be a group with n elements $a_1, a_2, ..., a_n$. A **multiplication table** for G is the $n \times n$ matrix with i, j entry $a_i * a_j$. Notice that a table depends on the ordering of the elements in G, and e is usually listed first.

Compare the 2 tables for groups $\{1,-1\}$ under multiplication and $\{0,1\}$ under addition modulo 2:

$$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

It is apparent that there is no significant difference between them.

Let $(G,*)$ and $(H,\circ)$ be groups (or semigroups).

A function $f: G \to H$ is a **homomorphism** if for all $a,b \in G$, $f(a*b) = f(a) \circ f(b)$.

An **isomorphism** is a homomorphism that is also a bijection.

G is isomorphic to H, denoted by $G \cong H$, if there exists an isomorphism $f: G \to H$.

The above 2 groups are isomorphic: $1 \mapsto 0$ and $-1 \mapsto 1$.

Essentially, 2 groups are isomorphic if their table 'match' when superimposed on each other.

In group theory, the 2 important problems are classifying groups: when are two groups isomorphic; and classifying transformations: describe all the homomorphism from one group to another.

Theorem 1.13 *Let $f: (G,*) \to (G',\circ)$ be a homomorphism. Then, $f(e) = e'$; If $a \in G$, then $f(a^{-1}) = f(a)^{-1}$; If $a \in G$ and $n \in \mathbb{Z}$, then $f(a^n) = f(a)^n$.*

Proof. $f(e) = f(e) \circ f(e) \circ f(e)^{-1} = f(e*e) \circ f(e)^{-1} = f(e) \circ f(e)^{-1} = e'$

$e' = f(e) = f(a*a^{-1}) = f(a) \circ f(a^{-1})$; From uniqueness of inverse (Theorem 1.10), $f(a^{-1}) = f(a)^{-1}$

By induction, $f(a^n) = f(a) \circ f(a^{n-1}) = f(a)^n$ $(n \geq 0)$; $f(a^{-n}) = f((a^{-1})^n) = f(a^{-1})^n = f(a)^{-n}$

Examples: $sgn: S_n \to \{\pm 1\}$ (Theorem 1.6); $v: \mathbb{Z} \to \mathbb{Z}_n$, defined by $v(a) = [a]$; $det: \mathrm{GL}(n,k) \to k^\times$

EXERCISES

1. (i) Write a multiplication table for S_3.

$$\left(\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right.$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right)$$

(ii) Show that S_3 is isomorphic to the group of Exercise 1.6.14.

From computations in (1.6.14), the functions in that group distinctly permute $\{0,1,\infty\}$.

Map each function to the permutation it corresponds; it is a bijection since the permutations are distinct.

2. Let $f: X \to Y$ be a bijection between sets X and Y. Show that $\alpha \mapsto f \circ \alpha \circ f^{-1}$ is an isomorphism $S_X \to S_Y$

Let g be the latter function. $g(\alpha \circ_X \beta) = f \circ \alpha \circ_X \beta \circ f^{-1} = f \circ \alpha \circ f^{-1} \circ_Y f \circ \beta \circ f^{-1} = g(\alpha) \circ_Y g(\beta)$

how to prove bijection?

3. Isomorphic groups have the same number of elements. Prove that the converse is false using $\mathbb{Z}_4$ and $\mathbb{V}$.

$(\forall a \in \mathbb{V})\ \ a^2 = e$; so an isomorphism $f : \mathbb{V} \to \mathbb{Z}_4$ must satisfy $f(a)^2 = e'$.

However not all $b \in \mathbb{Z}_4$ satisfy $b^2 = e'$; therfore an isomorphism doesn't exist.

4. If isomorphic groups are regarded as being the same, prove, for each $n \in \mathbb{N}$, that there are only finitely many distinct groups with n elements.

Consider the multiplication table A for a group G of n elements.

Each $A_{i,j}$ only has at most n choices, so the number of possible tables is at most n^{n^2}.

Since the number of possible groups are finite, there are only finitely many distinct groups.

5. Let $G = \{x_1, ..., x_n\}$ be a set equipped with an operation $*$, A be its multiplication table and assume G has a two-sided identity e.

(i) Show that $*$ is commutative iff A is a symmetric matrix.

By definition, $A_{i,j} = A_{j,i} \iff x_i * x_j = x_j * x_i$

(ii) Show that $\forall x \in G$ has a two-sided inverse iff A is a **Latin square** (no $x \in G$ is repeated in any row or column)

If first condition holds, let $x_i * x_j = e = x_j * x_i$;

$(\forall x_k \in G)\ \ x_k = x_i * x_j * x_k = x_i * L_{x_j}(x_k) \implies A_{i,L_{x_j}(x_k)} = k$

Since L_{x_j} is a bijection (1.6.10), the ith row is a permtation of G.

Similarly, $x_k = R_{x_j}(x_k) * x_j$ and $A_{R_{x_j}(x_k),j} = k$, so jth column is a permutation of G.

The converse is false; consider the following table:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

(iii) Assume that $e = x_1$. Show that $A_{i,1} = x_i^{-1}$ for all i iff $A_{i,i} = e$ for all i.

If $A_{i,i} = e$, $x_i * x_i = e$ so $A_{i,1} = x_i = x_i^{-1}$

If $A_{i,1} = x_i = x_i^{-1}$, $A_{i,i} = x_i * x_i = x_i * x_i^{-1} = e$

(iv) With the multiplication table as in (iii), show that $*$ is associative iff $A_{i,j}A_{j,k} = A_{i,k}$ for all i, j, k.

If $A_{i,j}A_{j,k} = A_{i,k}$, $(x_i * x_j) * (x_j * x_k) = x_i * x_k$

$\therefore (x * y) * z = (x * y) * (e * z) = (x * y) * ((e * y) * (y * z)) = (x * y) * (y * (y * z)) = x * (y * z)$

If $*$ is associative, $(x_i * x_j) * (x_j * x_k) = x_i * (x_j * x_j) * x_k = x_i * x_k$

6. (i) If $f : G \to H$ and $g : H \to K$ are homomorphisms, then so is the composite $g \circ f : G \to K$.

$g \circ f(x *_G y) = g(f(x) *_H f(y)) = g(f(x)) *_K g(f(y))$

(ii) If $f : G \to H$ is an isomorphism, then its inverse $f^{-1} : H \to G$ is also an isomorphism.

$f(x *_G y) = f(x) *_H f(y) \implies f^{-1}(f(x *_G y)) = f^{-1}(f(x) *_H f(y)) \implies$

$x *_G y = f^{-1}(f(x) *_H f(y)) \implies f^{-1}(f(x)) *_G f^{-1}(f(y)) = f^{-1}(f(x) *_H f(y))$

Since isomorphic, $\{f(x) \mid x \in G\} = \{y \mid y \in H\}$ so $f^{-1}(x' *_H y') = f^{-1}(x') *_G f^{-1}(y)$

(iii) If $\mathscr{C}$ is a class of groups, show that the relation of isomorphism is an equivalence relation on $\mathscr{C}$.

Every group has an isomorphism $x \mapsto x$ to itself;

From (ii), if isomorphism $f : G \to H$ exist, isomorphism $f^{-1} : H \to G$ exists

From (i), the compositions of isomorphisms is a homomorphism

and it is isomorphic because composition of bijections is a bijection

7. Let G be a group, X be a set and $f : G \to X$ be a bijection. Show that there is a unique operation on X so that X is a group and f is an isomorphism.

$\forall a, b \in X$ define $a * b = f(f^{-1}(a) *_G f^{-1}(b))$. It is associative so X is a semigroup.

From Theorem 1.13, X has an identity and inverses; thus X is a group.

Define a different operation $\circ$ where $\exists c, d \in X$ such that $c \circ d \neq c * d$.

Then $f^{-1}(c) *_G f^{-1}(d) = f^{-1}(c * d) \neq f^{-1}(c \circ s)$, so f is not an isomorphism with $\circ$.

8. If k is a field, denote the columns of the $n \times n$ identity matrix I by $\epsilon_1, ..., \epsilon_n$. A **permutation matrix** P over k is a matrix with columns being $\epsilon_{\alpha_1}, ..., \epsilon_{\alpha_n}$ for some $\alpha \in S_n$. Prove that the set of all permutation matrices over k is a group isomorphic to S_n.

Matrix multiplication is associative; $\forall P \;\; IP = P$ and $P^T P = I$ By Theorem 1.13 its a group

Define the isomorphism f as in the definition above (permutation of columns)

Since matrices multiply row by column, PQ represents the permutation from P^T to Q.

Let p, q, p^{-1}, q^{-1} be $f^{-1}(P), f^{-1}(Q), f^{-1}(P^T), f^{-1}(Q^T)$

P^T to Q means $q(p(p^{-1})) = q$ so the permutation PQ represents is $q \circ p$

Therefore group of permutation matrices is isomorphic to S_n ($q \circ p$ uses prefix notation)

9. Let $\mathbb{T}$ denote the **circle group**: the multiplicative group of all complex numbers of absolute value 1. For a fixed real number y, show that $f_y : \mathbb{R} \to \mathbb{T}$ given by $f_y(x) = e^{iyx}$, is a homomorphism.

$f_y(a + b) = e^{iy(a+b)} = e^{iya} e^{iyb} = f_y(a) f_y(b)$

10. (i) If a is a fixed element of a group G, define **conjugation** by a as $\gamma_a(x) = a * x * a^{-1}$ Prove that γ_a is an isomorphism.

From (1.6.10), L_a and R_a are isomorphisms so $\gamma_a = L_a \circ R_a$ is an isomorphism

(ii) If $a, b \in G$ prove that $\gamma_a\gamma_b = \gamma_{a*b}$.

$\gamma_a\gamma_b = L_aR_aL_bR_b = L_aL_bR_aR_b$ (1.6.10(iii)) $= L_{a*b}R_{a*b}$ (1.6.10(ii)) $= \gamma_{a*b}$

11. If G denotes the multiplicative group of all complex nth roots of unity then $G \cong \mathbb{Z}_n$.

Bijection $[k] \mapsto e^{i\pi k/n}$; $e^{i\pi[x]/n}e^{i\pi[y]/n} = e^{i\pi(x+y)/n} = e^{i\pi[x+y]/n}$

12. Describe all the homomorphisms from $\mathbb{Z}_{12}$ to itself. Which of these are isomorphisms?

Let $f(1) = x$. Then $f(n) = f(1 + ... + 1) = f(1) + ... + f(1) = nx$.

Therefore there are 12 possible homomorphisms for 12 choices of x.

Out of them $x = 1, 5, 7, 11$ are isomorphisms.

13. (i) Prove that a group G is abelian iff $f : G \to G$ defined by $f(a) = a^{-1}$ is a homomorphism.

$a * b * (a * b)^{-1} = 1 \implies b * (a * b)^{-1} = a^{-1} \implies (a * b)^{-1} = b^{-1} * a^{-1}$

$f(a * b) = f(a) * f(b) \implies (a * b)^{-1} = a^{-1} * b^{-1}$ Therefore $a^{-1} * b^{-1} = b^{-1} * a^{-1}$

(ii) Let $f : G \to G$ be an isomorphism from a finite group G to itself. If f has no nontrivial fixed points ($f(x) = x \implies x = e$) and if $f \circ f$ is the identity function, then $f(x) = x^{-1}$ for all $x \in G$ and G is abelian.

$f(f(x) * x) = f(f(x)) * f(x) = f(x) * x \implies f(x) * x = e \implies f(x) = x^{-1}$

From (i), G is abelian.

14. An element a in a ring R has a **left quasi-inverse** if there exists an element $b \in R$ with $a + b - ba = 0$. Prove that if every element in a ring R except 1 has a left quasi-inverse, then R is a division ring.

Define $f(x) = 1 - x$; $f(a + b - ba) = 1 - a - b + ba = (1 - b)(1 - a) = f(b)f(a)$

$a + b - ba = 0 \implies f(a + b - ba) = f(0) \implies f(b)f(a) = 1 \implies f(a)^{-1} = f(b)$

Since f is a bijection from $R - \{1\} \to R - \{0\}$, R is a division ring.

15. (i) If G is the multiplicative group of all positive real numbers, show that $\log : G \to (\mathbb{R}, +)$ is an isomorphism.

$\forall x \in \mathbb{R}^+ \ \ e^{\log x} = x$ and $\forall x \in \mathbb{R} \ \ \log e^x = x$ so log is a bijection and an isomorphism.

(ii) Let G be the additive group of $\mathbb{Z}[x]$ (all polynomials with integer coefficients) and let H be the multiplicative group of all positive rational numbers. Prove that $G \cong H$.

$\forall r \in \mathbb{R}^+ \ \ r = 2^{a_1}3^{a_2}5^{a_3}...$ where $a_i \in \mathbb{Z}$; define $f : \mathbb{R}^+ \to \mathbb{Z}[x]$ as $f(r) = a_1x + a_2x^2 + a_3x^3...$

Since it is a unique representation f is a bijection; $f(rs) = f(r) + f(s)$ so $G \cong H$.

2 The isomorphism theorems

2.1 Subgroups

A nonempty subset S of a group G is a **subgroup** of G if $s \in H$ implies $s^{-1} \in H$ and $s, t \in H$ implies $st \in H$.

If X is a subset of a group G, we write $X \subset G$; if X is a subgroup of G, we write $X \leq G$.

Theorem 2.1 *If $S \leq G$, then S is a group.*

Proof. "$s, t \in S \implies st \in S$" means that S is equipped with operation $\mu|S \times S$ where $\mu : G \times G \to G$

and that $\mu|S \times S$ has its image contained in S.

This operation on S is associative because it is associative for every element in G.

Since S is nonempty, $s \in S \implies s^{-1} \in S \implies ss^{-1} = 1 \in S$

Verifying associativity is the most tedious part of showing that a given set G equipped with an operation is actually a group. Therefore, if G is given as a subset of a group G^*, it is much simpler to show that G is a subgroup of G^*.

Theorem 2.2 *A subset S of a group G is a subgroup iff $1 \in S$ and $s, t \in S$ implies $st^{-1} \in S$.*

Proof. If $s \in S$, then $1s^{-1} = s^{-1} \in S$; if $s, t \in S$, then $s(t^{-1})^{-1} = st \in S$ (converse is easy)

If G is a group and $a \in G$, then the **cyclic subgroup generated by** a, denoted by $\langle a \rangle$, is the set of all the powers of a.

A group G is called **cyclic** if there is $a \in G$ with $G = \langle a \rangle$.

If G is a group and $a \in G$, then the **order** of a is $|\langle a \rangle|$, the number of elements in $\langle a \rangle$.

Theorem 2.3 *If G is a group and $a \in G$ has finite order m, then m is the smallest positive integer such that $a^m = 1$.*

Proof. If $a = 1$, then $m = 1$. If $a \neq 1$, there is an integer $k > 1$ so that $1, a, a^2, ..., a^{k-1}$ are distinct elements while $a^k = a^i$ for some $0 \leq i < k$.

If $a^k = a^i$ for some $1 \leq i < k$, $a^{k-i} = 1$ and $k - i > 0$, contradicting $1, a, a^2, ..., a^{k-1}$ has no repetitions. Therefore the smallest integer k that $a^k = a^i$ satisfies $a^k = 1$.

It now suffices to prove that $m = k$. Clearly $\{1, a, a^2, ..., a^{k-1}\} \subset \langle a \rangle$.

Let $l = qk + r$ where $0 \leq r < k$. $a^l = a^{qk+r} = a^r$ so $a^l = a^r \in \{1, a, a^2, ..., a^{k-1}\}$.

Since $\langle a \rangle$ is defined as the set of a^l, $\langle a \rangle \subset \{1, a, a^2, ..., a^{k-1}\}$. Therefore $\langle a \rangle = \{1, a, a^2, ..., a^{k-1}\}$ and $m = k$.

If $\alpha \in S_n$ is written as a product of t disjoint r_i-cycles, (1.2.9(iii)) shows that the order of α is $lcm(r_1, ..., r_t)$.

Corollary 2.4 *If G is a finite group, then a nonempty subset S of G is a subgroup iff $s, t \in S$ implies $st \in S$.*

Proof. Necessity is obvious. By induction S contains all the powers of s.

Since G is finite, s has a finite order m. Therefore $s^{-1} = s^{m-1} \in S$.

If G is a group, then G and $\{1\}$ (the **trivial** subgroup) are always subgroups.

Any subgroup H other than G is called **proper** ($H < G$).

Let $f : G \to H$ be a homomorphism; define

$$\ker(f) = \{a \in G : f(a) = 1\} \quad \text{im}(f) = \{h \in H : \exists a \in G \;\; h = f(a)\}$$

Then $\ker(f) \leq G$ and $\text{im}(f) \leq H$. $(f(st^{-1}) = f(s)f(t)^{-1} = 1$ and $uv^{-1} = f(f^{-1}(u)f^{-1}(v)^{-1}))$

Theorem 2.5 *The intersection of any family of subgroups of a group G is again a subgroup of G.*

Proof. Let $\{S_i : i \in I\}$ be a family of subgroups. $(\forall i \in I)\ 1 \in S_i$ so $1 \in \bigcap S_i$

If $a, b \in \bigcap S_i$, then $ab^{-1} \in S_i$ for all i, so $ab^{-1} \in \bigcap S_i$ and thus $\bigcap S_i \leq G$.

Corollary 2.6 *If X is a subset of G, then there is a **smallest** subgroup H of G containing X.*

Proof. $X \leq G$, so there are subgroups of G that contains X.

Define H as the intersection of all subgroups that contain X. By Theorem 2.5, $H \leq G$.

If $S \leq G$ and $X \subset S$, then S is one of the subgroups intersected to form H so $H \leq S$.

Therefore H is the smallest subgroup containing X.

The smallest subgroup of G containing X, $\langle X \rangle$, is called the **subgroup generated by** X.

If H and K are subgroups of G, the subgroup $\langle H \cup K \rangle$ is denoted by $H \vee K$.

If X is a nonempty subset of a group G, then a **word** on X is an element $w \in G$ of the form

$w = x_1^{e_1} x_2^{e_2} ... x_n^{e_n}$ where $x_i \in X$, $e_i = \pm 1$ and $n \geq 1$. (x_i need not be distinct)

Theorem 2.7 *Let X be a subset of a group G. If $X = \varnothing$, then $\langle X \rangle = \{1\}$; else $\langle X \rangle$ is the set of all the words on X.*

Proof. If $X = \varnothing$, the smallest possible subgroup $\{1\}$ contains X, so $\langle X \rangle = \{1\}$.

Let W be the set of all words. Since $x_1^{-1} x_1 = 1 \in W$ and $(\forall v, w \in W)\ vw^{-1} \in W$, $W \leq G$.

Since $\langle X \rangle$ is the smallest subgroup containing X and $X \subset W$, $\langle X \rangle \subset W$

Every subgroup H containing X must contain every word on X, so $W \leq H$. Therefore $\langle X \rangle = W$.

EXERCISES

1. Show that A_n, the set of all even permutations in S_n, (called the **alternating group** on n letters), is a subgroup with $n!/2$ elements.

From (1.6.6(i)), $(1\ 2\ ...\ r-1\ r)^{-1} = (r\ r-1\ ...\ 2\ 1)$, so the number of disjoint cycles of the inverse of an even permutation is the same as that of itself. Therefore $(\forall a \in A_n)\ sgn(a^{-1}) = sgn(a)$

Therefore $(\forall a, b \in A_n)\ sgn(ab^{-1}) = sgn(a)sgn(b^{-1}) = sgn(a)sgn(b) = 1 \times 1 = 1$

Therefore $A_n \leq S_n$ and from (1.4.3) A_n has $n!/2$ elements.

2. If k is a field, show that $\text{SL}(n, k)$, the **special linear group** over k, the set of all $n \times n$ matrices over k having determinant 1, is a subgroup of $\text{GL}(n, k)$.

Since $\det(A)\det(B) = \det(AB)$ and $\det(A)\det(A^{-1}) = \det(I)$,

if $a, b \in \mathrm{SL}(n,k)$ then $ab^{-1} \in \mathrm{SL}(n,k)$ so $\mathrm{SL}(n,k) \leq \mathrm{GL}(n,k)$

3. The set theoretic union of two subgroups is a subgroup iff one is contained in the other. Is this true if we replace "two subgroups" by "three subgroups"?

Let a, b be elements and G, H be subgroups such that $a \in G, a \notin H, b \in H, b \notin G$.

If $ab \in G$, then $a^{-1}ab \in G$, but $a^{-1}ab = b \notin G$, so $ab \notin G$ and similarly $ab \notin H$.

However, consider group $\{0, ..., 7\}$ with bitwise xor operation, and subgroups $\{0, 1, 6, 7\}$,

$\{0, 2, 5, 7\}, \{0, 3, 4, 7\}$; the union is a subgroup. Therefore the statement is no longer true.

4. Let S be a proper subgroup of G. If $G - S$ is the complement of S, prove that $\langle G - S \rangle = G$.

Let $a \in S$ and $b \in G$ but $b \notin S$. If $ab \in S$, $a^{-1}ab \in S$ but $a^{-1}ab = b \notin S$.

$b, ab \in G - S$, so $abb^{-1} = a \in \langle G - S \rangle$. Therefore $a \in S$ implies $a \in \langle G - S \rangle$, so $\langle G - S \rangle = G$.

5. Let $f, g : G \to H$ be homomorphisms and let $K = \{a \in G : f(a) = g(a)\}$. Must $K \leq G$?

If $a, b \in K$, $f(ab^{-1}) = f(a)f(b)^{-1} = g(a)g(b)^{-1} = g(ab^{-1})$ so $ab^{-1} \in K$ so $K \leq G$.

6. Suppose that X is a nonempty subset of a set Y. Show that S_X can be **imbedded** in S_Y; that is, S_X is isomorphic to a subgroup of S_Y.

too hard for me rn, google says need concepts after this or betrands postulate or smth

7. (i) Prove that S_n can be generated by $(1\ 2), (1\ 3), ..., (1\ n)$.

For any permutation $\beta \in S_n$, start with identity permutation $\alpha = 1_n$.

Repeat procedure: find $i \neq j$ s.t. $\alpha[i] = \beta[j]$; then $\alpha := (1\ i)(1\ j)\alpha$

(ii) Prove that S_n can be generated by $(1\ 2), (2\ 3), ..., (n-1\ n)$

Since $(1\ i) = (1\ 2)(2\ 3)...(i-1\ i)$, do the same procedure as above.

(iii) Prove that S_n can be generated by $\tau = (1\ 2)$ and $\rho = (1\ 2\ ...\ n)$.

Since $(i\ i+1)$ is $\rho^{n-i}\tau\rho^i$, do the same procedure as above.

(iv) Prove that S_4 cannot be generated by $\alpha = (1\ 3)$ and $\beta = (1\ 2\ 3\ 4)$.

Let $f_1(\gamma) = |\gamma[1] - \gamma[3]|$ and $f_2(\gamma) = |\gamma[2] - \gamma[4]|$ for $\gamma \in S_4$.

Then $f_1(\alpha) = f_2(\alpha) = f_1(\beta) = f_2(\beta) = f_1(1_4) = f_2(1_4) = 2$ so for all $\delta \in \langle \alpha, \beta \rangle$, $f_1(\delta) = 2$.

However, $f_1((1\ 2)) = 1$, so S_4 cannot be generated by α and β.

2.2 Lagrange's Theorem

If $S \leq G$ and $t \in G$, a **right coset** and a **left coset** of S in G are subsets of G

$$St = \{st : s \in S\} \quad tS = \{ts : s \in S\}$$

t is called the **representative** of St and tS.

In the additive group of $\mathbb{R}^2$, $l = \{r\vec{v} : r \in \mathbb{R}\}$ is a subgroup, and $\vec{u} + l$ is a coset.

In the additive group $\mathbb{Z}$ of all integers, the coset $a + \langle n \rangle$ is the congruence class $[a]$ of a mod n.

Not only is t a representative of St, every element st for $s \in S$ is a representative of St.

Lemma 2.8 *If $S \leq G$, then $Sa = Sb$ iff $ab^{-1} \in S$ (and $aS = bS$ iff $b^{-1}a \in S$).*

Proof. If $Sa = Sb$, then $a = 1a \in Sa = Sb$ so there is $s \in S$ with $a = sb$, hence $ab^{-1} \in S$.

Assume $ab^{-1} \in S$, then if $x \in Sa$, $x = sa = sab^{-1}b \in Sb$;

If $y \in Sb$, $y = s'b = s'ba^{-1}a = s(ab^{-1})^{-1}a \in Sa$, so $Sa = Sb$.

Theorem 2.9 *If $S \leq G$, any 2 right (or any 2 left) cosets of S in G are either identical or disjoint.*

Proof. If $\exists x \;\; x \in Sa \cap Sb$, $x = sb = ta$ where $s, t \in S$. Hence $ab^{-1} = t^{-1}s \in S$.

By Lemma 2.8 , $Sa = Sb$.

From above, the right cosets of a subgroup S comprise a partition of G.

For equivalence relation $a \equiv b$ if $ab^{-1} \in S$, its equivalence classes are the right cosets of S.

Theorem 2.10 *If $S \leq G$, then the number of right cosets of S in G is equal to the number of left cosets of S in G.*

Proof. Let $f : \mathscr{R} \to \mathscr{L}$ be $f(Sa) = a^{-1}S$. It is trivially a bijection.

($f(Sa) = aS$ is not well-defined because $Sa = Sb \implies ab^{-1} \in S \not\implies ba^{-1} \in S \implies aS = bS$)

If $S \leq G$, the **index** of S in G, denoted by $[G : S]$, is the number of right cosets of S in G.

From P. Hall (1935), in a finite group G, one can always choose a **common system of representatives** for the right and left cosets of a subgroup S; if $[G : S] = n$, there exist elements $t_1, ..., t_n \in G$ s.t. $t_1S, ..., t_nS$ and $St_1, ..., St_n$ is the family of all left and right cosets.

Theorem 2.11 (Lagrange but prolly Galois) *If G is a finite group and $S \leq G$, then $|S|$ divides $|G|$ and $[G : S] = |G|/|S|$*

Proof. By Theorem 2.9, G is partitioned into right cosets: $G = St_1 \cup St_2 \cup ... \cup St_n$

$f_i : S \to St_i$, defined by $f_i(s) = st_i$, is a bijection so $|St_i| = |S|$ for all i. Therefore $|G| = [G : S]|S|$.

Corollary 2.12 *If G is a finite group and $a \in G$, then the order of a divides $|G|$.*

Proof. Order of a is $|\langle a \rangle|$, and $\langle a \rangle \leq G$, so from Theorem 2.11 the order of a divides $|G|$.

A group G has **exponent** n if $x^n = 1$ for all $x \in G$.

Lagrange's theorem shows that a finite group G of order n has exponent n.

Corollary 2.13 *If p is a prime and $|G| = p$, then G is a cyclic group.*

Proof. Take $a \in G$ with $a \neq 1$. The cyclic subgroup $\langle a \rangle$ has more than 1 element.

From Corollary 2.12, $|\langle a \rangle|$ divides p, so $|\langle a \rangle| = p = |G|$, so $\langle a \rangle = G$

Corollary 2.14 (Fermat) *If p is a prime and a is an integer, then $a^p \equiv a \mod p$*

Proof. Let $G = U(\mathbb{Z}_p)$, the multiplicative group of nonzero elements of $\mathbb{Z}_p$

For integers a and b, $a \equiv b \mod p$ iff $[a] = [b]$ in $\mathbb{Z}_p$. If $[a] = [0]$, $[a]^p = [0] = [a]$.

If $[a] \neq [0]$, then $[a] \in G$ so $[a]^{|G|} = [a]^{p-1} = [1]$. $\therefore a^p \equiv a \mod p$.

EXERCISES

1. If G is a finite group and $K \leq H \leq G$, then $[G : K] = [G : H][H : K]$.

   $[G : K] = |G|/|K| = |G|/|H| \times |H|/|K| = [G : H][H : K]$

2. Let $a \in G$ have order $n = mk$ where $mk \geq 1$. Prove that a^k has order m.

   $1 = a^n = a^{mk} = (a^k)^m$

3. (i) Prove that every group G of order 4 is isomorphic to either $\mathbb{Z}_4$ or the 4-group $\mathbb{V}$.

   If there exist $a \in G$ such that $|\langle a \rangle| = 4$, $G \cong \mathbb{Z}_4$

   Else, $G = \{1, a, b, c\}$ where $a^2 = b^2 = c^2 = 1$.

   Then, $ab = c$ because otherwise $1 \neq a \neq b$ would be false.

   Similarly, $ba = c, ac = b, ca = b, bc = a, cb = a$ so $G \cong \mathbb{V}$.

(ii) If G is a group with $|G| \leq 5$, then G is abelian.

   If $|G| = 2, 3, 5$, $|\langle a \rangle| = 1$ or $|G|$ by Lagrange's theorem, so G must be cyclic.

   $\{1\}$, cyclic groups and $\mathbb{V}$ are all abelian.

4. If $a \in G$ has order n and k is an integer with $a^k = 1$, then n divides k. Indeed, $\{k \in \mathbb{Z} : a^k = 1\}$ consists of all the multiples of n.

   By definition, order n is the smallest integer s.t. $a^n = 1$. $\therefore 1 = (a^n)^m = a^{nm} = a^k$

   If $k = nm + r$ where $0 < r \leq n$, $a^k = a^{nm}a^r = a^r \neq 1$.

5. If $a \in G$ has finite order and $f : G \to H$ is a homomorphism, then the order of $f(a)$ divides the order of a.

   $f(a)^{|\langle a \rangle|} = f(a^{|\langle a \rangle|}) = f(1) = 1$. From 4., $|\langle a \rangle|$ is a multiple of $|\langle f(a) \rangle|$.

6. Prove that a group G of even order has an odd number of elements of order 2 (in particular, it has at least 1 such element).

   There is an even number of order > 2 elements because they can be paired into (x, x^{-1}).

   Subtracting that and 1 more (identity), there is an odd number of elements of order 2.

7. If $H \leq G$ had index 2, then $a^2 \in H$ for every $a \in G$.

$a \in H \implies a^2 \in H \therefore a^2 \notin H \implies a \notin H$

Since $[G : H] = 2$, $Ha = Ha^2 \implies H = Ha$ but they are different cosets.

Therefore the assumption that there exists $a^2 \notin H$ is wrong so $a^2 \in H$ for every a.

8. (i) If $a, b \in G$ commute and $a^m = 1 = b^n$, then $(ab)^k = 1$, where $k = lcm(m, n)$. Conclude that if a and b have finite order, then ab also has finite order.

$(ab)^k = a^k b^k = a^{mx} b^{ny} = 1$.

a, b finite order $\implies \exists a^m = 1 = b^n \implies \exists (ab)^k = 1 \implies ab$ finite order.

(ii) Let $G = \mathrm{GL}(2, \mathbb{Q})$, $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$. Show that $A^4 = I = B^3$ but AB has infinite order.

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, B^2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, A^4 = B^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, (AB)^n = \begin{bmatrix} 1 & 2^{n-1} \\ 0 & 1 \end{bmatrix}$$

9. Prove that every subgroup of a cyclic group is cyclic.

For any $a^i, a^j \in \langle a \rangle$, $\langle a^i, a^j \rangle = \langle a^g \rangle$ where $g = gcd(i, j)$.

This is because $\forall x, y \ (g \mid ix + jy)$ therefore $\langle a^i, a^j \rangle \subseteq \langle a^g \rangle$ and

$\exists z, w \ (iz + jw \equiv g)$ by Euclid's algorithm so $\forall n \ (gn = izn + jwn)$ so $\langle a^g \rangle \subseteq \langle a^i, a^j \rangle$

Since all subgroups are generated by some elements and those can be reduced to 1 element as shown above, all subgroups are generated by an element or in other words, cyclic.

10. Prove that two cyclic groups are isomorphic iff they have the same order.

If they are isomorphic there is a bijection so they have the same order;

if same order an isomorphism $f : \langle a \rangle \to \langle b \rangle$ such that $f(a) = b$ exists.

The **Euler ϕ-function** is defined as: $\phi(1) = 1$ and $\phi(n) = \sum_{k=1}^{n-1} [gcd(k, n) = 1]$ for $n > 1$

11. If $G = \langle a \rangle$ is cyclic of order n, then a^k is also a generator of G iff $gcd(k, n) = 1$. Conclude that the number of generators of G is $\phi(n)$.

$|\langle a^k \rangle|$ is the smallest integer such that $(a^k)^{|\langle a^k \rangle|} = 1$ so $n \mid k \times |\langle a^k \rangle|$ (4.)

$\therefore gcd(k, n) = 1 \iff |\langle a^k \rangle| = n$ and $\phi(n)$ is the number of generators of G.

12. (i) Let $G = \langle a \rangle$ have order rs where $gcd(r, s) = 1$. Show that there are unique $b, c \in G$ with b of order r, c of order s, and $a = bc$.

From steps in (9.), $\langle a^s, a^r \rangle = \langle a \rangle$ so $a^{sx} a^{ry} = a$ for some unique x, y (pigeon hole).

$|\langle a^{sx} \rangle| = n / gcd(n, sx) = r / gcd(r, x)$; similarly $|\langle a^{ry} \rangle| = s / gcd(s, y)$

$\because gcd(|\langle a^{sx} \rangle|, |\langle a^{ry} \rangle|) = 1 \therefore |\langle a^{sx} \rangle| |\langle a^{ry} \rangle| = |\langle a^{sx} a^{ry} \rangle| = |\langle a \rangle| = n$

Therefore $|\langle a^{sx} \rangle|$ and $|\langle a^{ry} \rangle|$ must be r and s respectively. $(b = a^{sx}, c = a^{ry})$

(ii) Prove that if $gcd(r, s) = 1$, then $\phi(rs) = \phi(r)\phi(s)$.

$gcd(k,n) = 1$ iff $gcd(k,r) = gcd(k,s) = 1$ and $a^k = b^k c^k$

so when a^k generates $\langle a \rangle$, b^k, c^k generates $\langle b \rangle, \langle c \rangle$; and $\langle a \rangle = \langle b \rangle \langle c \rangle$ so $\phi(rs) = \phi(r)\phi(s)$

13. (i) If p is prime, then $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

p is the only prime s.t. $p \mid p^k$ so there are $p^{k-1} - 1$ numbers (x) with $x < p^k$ and $gcd(p^k, x) \neq 1$

$\therefore \phi(p^k) = p^k - (p^{k-1} - 1) - 1 = p^k - p^{k-1} = p^k(1 - 1/p)$ (extra -1 from the identity)

(ii) If the distinct prime divisors of n are $p_1, ..., p_i$ then $\phi(n) = n(1 - 1/p_1), ..., (1 - 1/p_i)$.

Evident from (12. (ii)) and (13. (i))

14. If $gcd(r,s) = 1$, then $s^{\phi(r)} \equiv 1 \pmod{r}$.

$uv = 1 \pmod{r} \implies uv = 1 \pmod{p_1, ..., p_i} \implies u \neq 0 \pmod{p_1, ..., p_i} \implies gcd(u, r) = 1$

Since all u form a group $U(\mathbb{Z}_n)$ (example 1.6.4), $s^{\phi(r)} \equiv 1 \pmod{r}$ for all $s \in U(\mathbb{Z}_n)$.

2.3 Cyclic Groups

Lemma 2.15 *G is a cyclic group of order $n \implies \forall d|n$ ($\exists$ a subgroup of order d).*

Proof. $G = \langle a \rangle \implies |\langle a^{n/d} \rangle| = d$ (exercise 2.2.2)

Assume $S = \langle b \rangle$ is a subgroup of order d. S is cyclic. (exercise 2.2.9)

$b^d = 1$ and $\exists m\ b = a^m$. By (exercise 2.2.4), $\exists k\ md = nk \implies b = a^m = (a^{n/d})^k \implies \langle b \rangle \leq \langle a^{n/d} \rangle$. Since $|\langle b \rangle| = |\langle a^{n/d} \rangle| = d$, the inclusion is equality $\langle b \rangle = \langle a^{n/d} \rangle$.

Theorem 2.16 *If n is a positive integer, $n = \sum_{d|n} \phi(d)$*

Proof. If C is a cyclic subgroup of G, let $gen(C)$ denote the set of all its generators.

Since each element a generates a unique cyclic subgroup $\langle a \rangle$, $G = \bigcup gen(C)$.

From (lemma 2.15) each C is unique so $n = \sum_{d|n} |gen(C_d)| = \sum_{d|n} \phi(d)$.

Theorem 2.17 *A group G of order n is cyclic $\iff \forall d|n$ There is at most 1 cyclic subgroup of G with order d.*

Proof. Implication is proved in (lemma 2.15). From previous proof, $n = \sum |gen(C)|$.

Since there is at most 1 cyclic subgroup of order d, $n = \sum_{d|n} \phi(d) \times [C_d \in G]$

But from (theorem 2.16) $n = \sum_{d|n} \phi(n)$ so $\forall d\ \exists C_d \in G$

Therefore there exists a cyclic subgroup of order $d = n$ so G is cyclic.

Theorem 2.18 *If F is a field and G is a finite subgroup of $F^\times$, the multiplicative group of nonzero elements of F, then G is cyclic.*

Proof. If $|G| = n$ and $a \in G$ satisfies $a^d = 1$ $(d|n)$, then a is a root in F of $x^d - 1$.

Since a polynomial of degree d over a field has at most d roots (fundamental theorem of algebra), there is at most 1 cyclic subgroup of G having order d.

Therefore from (theorem 2.17) G is cyclic.

The proof is not constructive; no algorithm is known to display a generator of $\mathbb{Z}_p^\times$ for all primes.

Theorem 2.19 *Let p be a prime. A group G of order p^n is cyclic iff it is an abelian group having a unique subgroup H of order p.*

Proof. Necessity follows from lemma 2.15. For converse, let $a \in G$ have largest order p^k.

$\forall g \in G, |\langle g \rangle| = p^j$ where $j \leq k$ so $g^{p^k} = 1$. If $b \in G$ and $b^p = 1$, $b \in \langle b \rangle = H$ (or $b = 1 \in H$).

Let $w \in G$ but $w \notin \langle a \rangle$. At some point in $w, w^p, w^{p^2}, ..., w^{p^k} = 1$, $\exists i\ w^{p^i} \notin \langle a \rangle$ to $w^{p^{i+1}} \in \langle a \rangle$.

Let $x = w^{p^i}$ and $x^p = a^l$. If $k = 1$, $x^{p^k} = x^p = 1$ so $x \in H \leq \langle a \rangle$, a contradiction.

if $k > 1$, $1 = x^{p^k} = (x^p)^{p^{k-1}} = a^{lp^{k-1}}$, then $p^k | lp^{k-1}$ (exercise 2.2.4) so $\exists m \in \mathbb{Z}\ l = pm$.

Hence $x^p = a^l = a^{mp} \implies 1 = x^{-p}a^{mp} = (x^{-1}a^m)^p$ (abelian) $\implies x^{-1}a^m \in H \leq \langle a \rangle$, a contradiction.

Therefore there is no $w \in G$ s.t. $w \notin \langle a \rangle$ hence $G = \langle a \rangle$.

EXERCISES

1. Let $G = \left\langle \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle$. Show that G is a nonabelian group of order 8 having a unique subgroup of order 2.

Subgroup: $\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right)$ Representatives: $\left(\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \right)$

2.4 Normal Subgroups

If S and T are nonempty subsets of a group G, $ST = \{st : s \in S \wedge t \in T\}$.

The family of all nonempty subsets of G is a semigroup (it is associative).

Theorem 2.20 (Product Formula) *If S and T are subgroups of a finite group G, then $|ST||S \cap T| = |S||T|$*

Proof. Define $\phi : S \times T \to ST$ by $(s, t) \mapsto st$.

ϕ is a surjection so it suffices to show $x \in ST \implies |\phi^{-1}(x)| = |S \cap T|$.

Let $U = \{(sd, d^{-1}t) : d \in S \cap T\}$ where $st = x$. Clearly, $U \subseteq \phi^{-1}(x)$. Let $(s, t), (\sigma, \tau) \in \phi^{-1}(x)$.

Then $st = x = \sigma\tau \implies s^{-1}\sigma = t\tau^{-1} \in S \cap T \implies (\sigma, \tau) = (ss^{-1}\sigma, \tau t^{-1}t) = (s(s^{-1}\sigma), (s^{-1}\sigma)^{-1}t)$

Therefore $\phi^{-1}(x) \subseteq U$ and $\phi^{-1}(x) = U$ so $|S||T| = |ST||S \cap T|$.

A subgroup $K \leq G$ is a **normal subgroup**, denoted by $K \lhd G$, if $\forall g \in G\ gKg^{-1} = K$.

$K \leq G$ and $\forall g \in G\ (gKg^{-1} \leq K) \implies g^{-1}Kg \leq K \implies K \leq gKg^{-1} \implies K \lhd G$

$K \leq G$ and $\forall g \in G\ (Kg = gK) \iff K = Kgg^{-1} = gKg^{-1} \iff K \lhd G$

$a \in ker(f) \implies f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)f(g)^{-1} = 1 \implies gag^{-1} \in ker(f) \implies ker(f) \lhd G$

If $x \in G$ a **conjugate** of x in G is an element of the form axa^{-1} for some $a \in G$.

x and y are conjugate if $y = \gamma_a(x)$ for some $a \in G$.

For example, if k is a field, A and B in $GL(n, k)$ are conjugate $\iff$ they are similar.

EXERCISES

1. $S \leq G \implies SS = S$; $|S| \in \mathbb{N} \wedge SS = S \implies S \leq G$; Give an example to show the converse may be false when S is infinite.

If $S \leq G$, clearly $SS \subseteq S$; moreover $S = S1 \subseteq SS$. For the converse, $\forall a, b \in S\ (ab \in S)$;

$\forall a \neq b \neq c \in S$ if $ab = ac$, $a \in G \implies a^{-1} \in G \implies a^{-1}ab = a^{-1}ac \implies b = c$

Therefore $\forall a, b, c \in S\ (ab \neq ac) \implies$ if S is finite, $\forall x \in S\ (Sx = S) \implies \forall x \in S\ (x^{-1} \in S)$

Example: $\mathbb{N}$ in additive group of $\mathbb{Z}$ I just saw corollary 2.4 :(

2. Let $\{S_i : i \in I\}$ s.t. $S_i \leq G$ and let $D = \bigcap S_i$. Prove that either $\bigcap S_i t_i = \varnothing$ or $\bigcap S_i t_i = Dg$ for some g.

Let $x \in \bigcap S_i t_i$. $x \in Dg$ for some g and only $S_i g \supseteq Dg$ so $\bigcap S_i t_i = \bigcap S_i g = Dg$.

$\therefore \bigcap S_i t_i \neq \varnothing \implies \bigcap S_i t_i = Dg$

3. If $S, T \leq G$, then an **S-T-double coset** is a subset of G in the form SgT where $g \in G$. Prove that the family of all (S-T)-double cosets partitions G.

Define $a \equiv b$ if $\exists s \in S\ \exists t \in T\ (b = sat)$. $a = 1a1$; $b = sat \implies a = s^{-1}bt^{-1}$;

$b = s_1 a t_1 \wedge c = s_2 b t_2 \implies c = s_2 s_1 a t_1 t_2$. Therefore it is an equivalence relation.

4. Let $S, T \leq G$ where G is a finite group and $G = \bigcup_{i=1}^{n} Sg_iT$. Prove that $[G : T] = \sum_{i=1}^{n} [S : S \cap g_i T g_i^{-1}]$.

From product formula, $\sum_{i=1}^{n} |S|/|S \cap g_i T g_i^{-1}| = \sum_{i=1}^{n} |Sg_iTg_i^{-1}|/|g_iTg_i^{-1}| = 1/|T| \sum_{i=1}^{n} |Sg_iTg_i^{-1}|$

$= 1/|T| \sum_{i=1}^{n} |Sg_iT| = |G|/|T| = [G : T]$

5. (i) **(H. B. Mann)** Let G be a finite group and S, T be nonempty subsets. Prove that either $G = ST$ or $|G| \geq |S| + |T|$.

If $G = ST$, $\exists x$ s.t. $st \neq x$. $\forall a \in G\ \exists b \in G$ s.t. $ab = x$ and all the bs cover G.

$\therefore$ For each of the $|G|$ pairs (a, b), $a \in S \wedge b \in T$ is false. $\therefore |S| + |T| \leq |G| + |G| - |G| = |G|$

(ii) Prove that every element in a finite field F is a sum of two squares.

$\forall a \in F$ s.t. $a \neq 0$ there is at most 2 solutions to $x^2 = a$.

Therefore there is at most $\lceil (|F| - 1|)/2 \rceil + 1 > |F|/2$ squares.

Since number of squares$\times 2 > |F|$, the sum of two squares cover F by (i).

6. If $S \leq G$ and $[G : S] = 2$, then $S \lhd G$.

Let $x \in G$ s.t. $x \notin S$. If $sxtx \in Sx$ for some $s, t \in S$, $sxt \in S$ but $(Sx)S = (xS)S = xS = Sx$.

$\therefore SxSx = S$. If $g \in S$, $gSg^{-1} = S$. Else, $gSg^{-1} \subseteq SxSSx = SxSx = S$.

7. If G is abelian, then every subgroup of G is nromal. The converse is false: show that the group of order 8 in exercise 2.3.1 is a counterexample.

$\forall g \in G$ and some $S \leq G$, $gSg^{-1} = gg^{-1}S = S$;

$$g = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, g(\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) g^{-1} = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)$$

8. If $H \leq G$, then $H \lhd G \iff \forall x, y \in G\ (xy \in H \iff yx \in H)$.

$Hy^{-1}y = H$ and $xy \in H$ and $\{Hg : g \in G\}$ disjoint $\implies x \in Hy^{-1} \implies yx \in yHy^{-1}$

$\therefore H \lhd G \implies yx \in yHy^{-1} = H$

Fix $y \in G$. For the $|H|$ xs s.t. $xy \in H$, there are $|H|$ elements $yx \in yHy^{-1}$.

However all of them is in $H \implies \forall y\ (yHy^{-1} \leq H) \implies H \lhd G$

9. If $K \leq H \leq G$ and $K \lhd G$, then $K \lhd H$.

$\forall g \in G\ (gKg^{-1} = K) \implies \forall h \in H\ (hKh^{-1} = K)$

10. $S \lhd G \iff (s \in S \implies$ every conjugate of s in S (equivalently $\gamma(S) \leq S))$.

By definition

11. Prove that $SL(n, k) \lhd GL(n, k)$

For $s \in SL(n, k)$ and $g \in GL(n, k)$, $\det(gsg^{-1}) = \det(g)\det(s)\det(g^{-1}) = \det(g)\det(g)^{-1} = 1$

12. Prove that $A_n \lhd S_n$ for every n.

$[A_n : S_n] = 2$ so by (6)$A_n \lhd S_n$

13. (i) The intersection of any family of normal subgroups of a group G is itself a normal subgroup of G. If X is a subset of G, then there is a smallest normal subgroup of G which contains X called the **normal subgroup generated by** X, $\langle X \rangle^G$

Intersection of subgroups is a subgroup; $\forall g \in G$, $\forall s \in \bigcap S_i$ and $\forall S_i$, $gsg^{-1} \in S_i \therefore gsg^{-1} \in \bigcap S_i$

The smallest normal subgroup which contains X is the intersection of all subrgoup that contains X and G is also a normal subgroup.

(ii) $X = \varnothing \implies \langle X \rangle^G = 1$ else $\langle X \rangle^G$ is the set of all words on conjugates of elements in X.

Every normal subgroup that contains X must contain $\langle X \cup g_1 X g_1^{-1} \cup ... \cup g_n X g_n^{-1} \rangle$

And it is a normal group because $gg_1x_1g_1^{-1}g_2x_2g_2^{-1}...g_nxg_n^{-1}g^{-1} = g_1'x_1g_1^{-1}g_2x_2g_2^{-1}...g_nx_ng_n^{-1}$

$= g_1'x_1g_1'^{-1}gg_2x_2g_2^{-1}...g_nx_ng_n^{-1} = g_1'x_1g_1'^{-1}g_2'x_2g_2'^{-1}...g_n'x_ng_n'^{-1}$

(iii) If $gxg^{-1} \in X$ for all $x \in X, g \in G$, then $\langle X \rangle = \langle X \rangle^G \lhd G$.

$\langle X \rangle \ni x_1...x_n = g_1x_1'g_1^{-1}...g_nx_ng_n^{-1} \in \langle X \rangle^G \therefore \langle X \rangle = \langle X \rangle^G \lhd G$

14. If $H, K \lhd G$ then $H \vee K \lhd G$.

Proved like (13 (ii))

15. Prove that if a normal subgroup H of G has index n, then $g^n \in H$ for all $g \in G$. Give an exmaple to show this may be false when H is not normal.

Fix $g \in G$. Then G can be parititioned into disjoint sets $G = \bigcup_{i=1}^{x} \langle g \rangle s_i H$ $(s_i \in G)$ (3.).

$x = |G|/(|\langle g\rangle||H|) \Longrightarrow x|\langle g\rangle| = [G:H] \Longrightarrow g^n = 1 \in H$ for all $g \in G$

2.5 Quotient Groups

Theorem 2.21 *If $N \lhd G$, then the cosets of N in G form a group, denoted by G/N or order $[G:N]$.*

Proof. $NaNb = Na(a^{-1}Na)b = NNab = Nab$; identity is N and inverse of Na is Na^{-1}

Corollary 2.22 *If $N \lhd G$, then the **natural map** ($\nu : G \to G/N$ defined by $\nu(a) = Na$) is a surjective homomorphism with kernel N.*

Proof. Clearly ν is a homomorphism; $Na \in G/N \Longrightarrow Na = \nu(a)$ so ν is surjective; $\ker \nu = N$

If $a, b \in G$, the **commutator** of a and b, denoted by $[a, b]$, is $aba^{-1}b^{-1}$.

The **commutator subgroup** or derived subgroup of G, denoted G', is the subgroup of G generated by all the commutators.

Theorem 2.23 *$G' \lhd G$; if $H \lhd G$, then G/H is abelian $\Longleftrightarrow G' \leq H$.*

Proof. If $f : G \to G$ is a homomorphism, then $f(G') \leq G'$ because $f([a, b]) = [f(a), f(b)]$. From (2.4.10), $\gamma(G') \leq G' \Longrightarrow G' \lhd G$

If G/H abelian, then $HaHb = HbHa \Longrightarrow Hab = Hba \Longrightarrow Haba^{-1}b^{-1} = H$ therefore every commutator should be in H which implies $G' \leq H$ (because H is a group)

If $G' \leq H$, then $Haba^{-1}b^{-1} = H \Longrightarrow Hab = Hba \Longrightarrow HaHb = HbHa$

EXERCISES

1. Let $H \lhd G$, $\nu : G \to G/H$ be the natural map, and $x \subset G$ s.t. $\langle \nu(X)\rangle = G/H$. Prove that $G = \langle H \cup X\rangle$.

$\nu(X)$ generates all cosets of $H \Longrightarrow X$ generates all the representatives; $\therefore X \cup H$ generates G

2. Let G be a finite group of odd order, and let x be the product of all elements in some order. Prove that $x \in G'$.

Let $x = a_1...a_n$. To move a_j to position i, where $i < j$, one can do the following:

$x[(a_j...a_n)^{-1}, (a_i...a_{j-1})^{-1}] = (a_1...a_{i-1})(a_i...a_{j-1})(a_j...a_n)(a_j...a_n)^{-1}(a_i...a_{j-1})^{-1}(a_j...a_n)(a_i...a_{j-1})$

$= a_1...a_{i-1}a_j...a_n a_i...a_{j-1}$

Therefore, one can apply the procedure in increasing i to sort x into the form $a_1a_1^{-1}a_2a_2^{-1}... = 1$

Since multiplying by commutators ended up with 1, x itself must be in G'.

3. For any group G, show that $G' \subseteq \{a_1a_2...a_na_1^{-1}a_2^{-1}...a_n^{-1}\}$

$[a, b][c, d][e, f]... = aba^{-1}b^{-1}cdc^{-1}d^{-1}efe^{-1}f^{-1}...a^{-1}ab^{-1}bc^{-1}cd^{-1}de^{-1}ef^{-1}f...$

$= (a)(ba^{-1})(b^{-1})(c)(dc^{-1})(d^{-1})(e)(fe^{-1})(f^{-1})...(a^{-1})(ba^{-1})^{-1}(b)(c^{-1})(dc^{-1})^{-1}(d)(e^{-1})(fe^{-1})^{-1}(f)...$

4. (i) Let $k[x, y]$ denote the ring of all polynomials in 2 variables over a field k; let $k[x]$ and $k[y]$ denote subrings of all polynomials in x and y. Define G to be the set of all matrices of the form

$$A = \begin{bmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{bmatrix}$$

where $f(x) \in k[x], g(y) \in k[y], h(x, y) \in k[x, y]$. Prove that G is a multiplicative group and G'

consists of all those matrices for which $f(x) = g(y) = 0$.

$$\begin{bmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & f' & h' \\ 0 & 1 & g' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & f+f' & h+h'+fg' \\ 0 & 1 & g+g' \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -f' & -h'+f'g' \\ 0 & 1 & -g' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & f-f' & h-h'+f'g'-fg' \\ 0 & 1 & g-g' \\ 0 & 0 & 1 \end{bmatrix} \in G$$

$$[A, A'] = \begin{bmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & f' & h' \\ 0 & 1 & g' \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -f & -h+fg \\ 0 & 1 & -g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -f' & -h'+f'g' \\ 0 & 1 & -g' \\ 0 & 0 & 1 \end{bmatrix}$$

$\therefore [A, A']_{1,2} = f + f' - f - f' = 0$ and $[A, A']_{2,3} = g + g' - g - g' = 0$ so $G' \subseteq \{f, g = 0\}$

$$\left[\begin{bmatrix} 1 & f & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \right] = \begin{bmatrix} 1 & f & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -f & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -g \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & f & fg \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -f & fg \\ 0 & 1 & -g \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & fg \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\therefore \text{ if } h = \sum_{i,j} a_{i,j} x^i y^j \text{ then } \begin{bmatrix} 1 & 0 & h \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \prod_{i,j} \left[\begin{bmatrix} 1 & a_{i,j}x^i & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & y_j \\ 0 & 0 & 1 \end{bmatrix} \right] \text{ so } \{f, g = 0\} \subseteq G'$$

(ii) If $\begin{bmatrix} 1 & 0 & h \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is a commutator, then there are polynomials $f(x), f'(x), g(y), g'(y)$ s.t. $h = fg' - f'g$.

$$[A, A'] = \begin{bmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & f' & h' \\ 0 & 1 & g' \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -f & -h+fg \\ 0 & 1 & -g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -f' & -h'+f'g' \\ 0 & 1 & -g' \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & f+f' & h+h'+fg' \\ 0 & 1 & g+g' \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -f-f' & -h-h'+fg+f'g'+fg' \\ 0 & 1 & -g-g' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & fg'-f'g \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

(iii) Show that $h(x, y) = x^2 + xy + y^2$ does not possess a decomposition as in (ii), and that $\begin{bmatrix} 1 & 0 & x^2+xy+y^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is not a commutator.

Let $f(x) = \sum_{i=1}^{\infty} a_i x^i, f'(x) = \sum_{i=1}^{\infty} b_i x^i$. Since $h = fg' - f'g$,

$$\begin{cases} b_0 g'(y) - c_0 g(y) = 0 + 0y + y^2 \\ b_1 g'(y) - c_1 g(y) = 0 + y + 0y^2 \\ b_2 g'(y) - c_2 g(y) = 1 + 0y + 0y^2 \end{cases}$$

It is impossible that 3 linear combinations of 2 vectors to be orthogonal. Therefore it is not a commutator.

2.6 The Isomorphism theorems

There are 3 theorems formulated by E. Noether that desctibes the relationship between quotient groups, normal subgroups and homomorphisms. Analogues of them are true for most types of algebraic systems such as semigroups, rings, vector spaces, modules and operator groups.

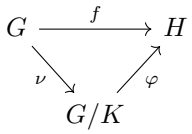
Theorem 2.24 (First Isomorphism Theorem) *Let $f : G \to H$ be a homomorphism with kernel K. Then $K \lhd G$ and $G/K \cong \operatorname{Im} f$.*

Proof. Define $\varphi : G/K \to H$ by $\varphi(Ka) = f(a)$. To see that it is well-defined, assume $Ka = Kb \iff$

$ab^{-1} \in K \iff 1 = f(ab^{-1}) = f(a)f(b)^{-1} \iff f(a) = f(b) \iff \varphi(Ka) = \varphi(Kb)$

φ is a homomorphism: $\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb)$. $\operatorname{Im}\varphi = \operatorname{Im} f$.

Finally, φ is an injection: $\varphi(Ka) = \varphi(Kb) \implies Ka = Kb$ from above. So φ is an isomorphism.



Lemma 2.25 *If $S, T \leq G$ and one of them is normal, then $ST = S \vee T = TS$*

Proof. Clearly $ST, TS \subseteq S \vee T$; If ST is a group, then $S \vee T \subseteq ST$ by definition.

Assume $T \lhd G$. $(s_1t_1)(s_2t_2)^{-1} = s_1s_2^{-1}s_2t_1t_2^{-1}s_2^{-1} = s_1s_2^{-1}t_3 \in ST$

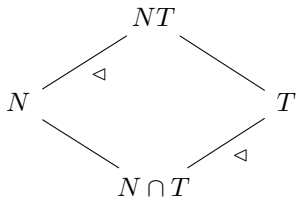
Similarly, $TS \leq G$ so $ST = S \vee T = TS$.

Theorem 2.26 (Second Isomorphism Theorem) *Let $N \lhd G, T \leq G$. Then $N \cap T \lhd T$ and $T/(N \cap T) \cong (NT)/N$.*

Proof. Let $\nu : G \to G/N$ be the natural map. Since $\ker(\nu|_T) = N \cap T$,

first isomorphism theorem gives $N \cap T \lhd T$ and $T/(N \cap T) \cong \operatorname{Im}(\nu|_T)$.

$\operatorname{Im}(\nu|_T)$ is the family of all cosets of N having a representative in T, or $(NT)/N$.



Theorem 2.27 (Third Isomorphism Theorem) *Let $K \leq H \leq G$ where $K, H \lhd G$. Then $H/K \lhd G/K$ and $(G/K)/(H/K) \cong G/H$.*

Proof. Define $f : G/K \to G/H$ by $f(Ka) = Ha$ (well-defined because $K \leq H$).

$\ker f$ is the cosets of K in H. By first isomorphism theorem, $H/K \lhd G/K$ and $(G/K)/(H/K) \cong G/H$.

EXERCISES

1. Prove that homomorphism $f : G \to H$ is an injection $\iff \ker f = 1$.

f injection $\iff \operatorname{Im} \cong H \cong G \iff G \cong G/K \iff K = 1$ 2. (i) Show that $\mathbf{V} \lhd S_4$.

There exists homomorphism $f : S_4 \to S_3$ with kernel $\mathbf{V} \implies \mathbf{V} \lhd S_4$.

(ii) If $K = \langle (1\ 2)(3\ 4) \rangle$ show that $K \lhd \mathbf{V}$ but $K \not\lhd S_4$. Conclude that normality need not be transitive.

K consists of 2 elements so by (2.4.6) $K \lhd \mathbf{V}$. $(1\ 3)(1\ 2)(3\ 4)(1\ 3) = (1\ 4)(2\ 3) \notin K$.

3. Let $N \lhd G$ and $f : G \to H$ be a homomorphism whose kernel contains N. Show that f induces a homomorphism $f_* : G/N \to H$ by $f_*(Na) = f(a)$.

$Na = Nb \iff ab^{-1} \in N \subseteq \ker f \iff 1 = f(ab^{-1}) = f(a)f(b)^{-1} \iff f(a) = f(b) \iff f_*(Na) = f_*(Nb)$

$\therefore f$ is well-defined and injective. Clearly f is a homomorphism.

4. If $S, T \leq G$ then $ST \leq G \iff ST = TS$.

$sT = Ts \implies sTs^{-1} = T$; $s_1t_1(s_2t_2)^{-1} = s_1s_2^{-1}s_2t_1t_2^{-1}s_2^{-1} = s_1s_2^{-1}t_3$. $\therefore ST = TS \implies ST \leq G$.

If $ST \leq G$, $s_1t_1t_2^{-1}s_2^{-1} = s_3t_3 \implies t_2^{-1}s_2^{-1} = t_1^{-1}s_1^{-1}s_3t_3 \implies t_5s_5 = t_4s_4(t_6s_6)^{-1} \implies TS \leq G$.

By Lemma 2.25, $ST = S \vee T = TS$.

5. **(Modular Law)** Let $A, B, C \leq G$ and $A \leq B$. If $A \cap C = B \cap C$ and $AC = BC$, then $A = B$.

$|A||C| = |AC||A \cap C| = |BC||B \cap C| = |B||C|$ so $|A| = |B|$ and $A \leq B$ therefore $A = B$.

6. **(Dedekind Law)** Let $H, K, L \leq G$ with $H \leq L$. Then $HK \cap L = H(K \cap L)$.

$\forall h \in H$, $h(K \cap L) = h(K \cap h^{-1}L) = hK \cap L$; $\therefore H(K \cap L) = HK \cap L$.

7. Let $f : G \to G^*$ be a homomorphism and $S^* \leq G^*$. Then $\ker f \subseteq \{x \in G : f(x) \in S^*\} \leq G$.

For x, y in the set, $f(xy^{-1}) = f(x)f(y)^{-1} \in S^*S^* = S^*$ so xy^{-1} is also in the set.

Therefore it is a subgroup, and $\ker f$ is clearly contained.

2.7 Correspondance theorem

This theorem should be called the fourth isomorphism theorem. Let X and X^* be sets. A function $f : X \to X^*$ induces a forward and a backward motion between subsets of X and subsets of X^*.

Forward motion assigns $S \subseteq X$ the subset $f(S) = \{f(s) : s \in S\}$ of X^*; backward motion assigns $S^* \subseteq X^*$ the subset $f^{-1}(S^*) = \{x \in X : f(x) \in S^*\}$ of X.

If f is a surjection, these motions define a bijection between all subsets of X^* and certain subsets of X.

Theorem 2.28 (Correspondance Theorem) *Let $K \lhd G$ and $\nu : G \to G/K$ be the natural map. Then $S \mapsto \nu(S) = S/K$ is a bijection from the family of all subgroups $S \leq G$ which contain K to the family of all the subgroups of G/K.*
If we denote S/K by S^*, then:
$T \leq S \iff T^* \leq S^*$, and then $[S : T] = [S^* : T^*]$;
$T \lhd S \iff T^* \lhd S^*$, and then $S/T \cong S^*/T^*$

Proof. We show first that $S \mapsto S/K$ is an injection: $S/K = T/K \implies S = T$.