Part 1A Groups - Theorems, Lemmas and Proofs

By Jack Fielding and Miren Radia

1 Basic Definitions and Examples

Lemma 1.1. *Let $(G, *)$ be a group, then,*
(i) The identity is unique.
(ii) The inverses are unique.

Proof. Suppose we have two identity elements e and e'. Then $\forall x \in G, x * e = x = x * e$ and $x * e' = x = e' * x$. Now $e = e' * e = e'$ so $e = e'$.
Given an element $g \in G$ suppose g has two inverses, h and h'. Then $g * h = e = h * g$ and $g * h' = e = h' * g$. Now $h = h * e = h * (g * h') = (h * g) * h' = e * h' = h'$. □

Lemma 1.2. *If $g : A \to B$ and $f : B \to C$ are both injective/surjective/bijective, then so is $f \circ g$.*

Proof. (i) $f(g(x)) = f(g(y)) \Rightarrow g(x) = g(y) \Rightarrow x = y$ since f and g are injective.
(ii) Given $z \in C \,\exists\, y \in B : f(y) = z$, but given any $y \in B \,\exists\, x \in A : g(x) = y$. So given $z \in C \,\exists\, x \in A : f(g(x)) = z$.
(iii) If f and g are both bijective this means $f \circ g$ is injective and surjective, so it is bijective. □

Lemma 1.3. *Let $(G, *_g)$ and $(H, *_h)$ be groups and $\theta : (G, *_g) \to (H, *_h)$ a homomorphism. Then $Im(\theta) = \theta(G) = \{\theta(g) : g \in G\}$ is a subgroup under $*_h$ of $(H, *_h)$.*

Proof. Given two elements $\theta(x)$ and $\theta(y)$, consider $\theta(x) *_h \theta(y) = \theta(x *_g y)$ which is in $Im(\theta)$. Now consider $\theta(x) *_h \theta(e_g) = \theta(x) = \theta(e_g) *_h \theta(x)$, so we have an identity, namely $\theta(e_g)$. Suppose we are given an element $\theta(g) \in Im(G)$ then consider $\theta(g) *_h \theta(g^{-1}) = \theta(g *_g g^{-1}) = \theta(e_g)$. So $\theta(g)^{-1} = \theta(g^{-1})$. Consider $(\theta(x) *_h \theta(y)) *_h \theta(y) = \theta((x *_h y) *_h z) = \theta(x *_h (y *_h z) = \theta(x) *_h (\theta(y) *_h \theta(z))$ □

Lemma 1.4. *(i) Let F, G and H all be groups and $\theta : G \to H$ and $\phi : F \to G$ both be homomorphisms/isomorphisms, then so is the composition $\theta \circ \phi$.*
(ii) Let F and G be groups (as above) and let $\phi : f \to G$ be an isomorphism. Then ϕ^{-1} is an isomorphism.

Proof. (i) Consider $(\theta \circ \phi)(x) *_h (\theta \circ \phi)(y) = \theta(\phi(x)) *_h \theta(\phi(y)) = \theta(\phi(x) *_g \phi(y)) = \theta(\phi(x *_f y)) = (\theta \circ \phi)(x *_f y)$ This proves the result for homomorphisms. The result for isomorphism requires also the composition to be a bijection, this is proved in Lemma 1.2.
(ii) Since ϕ is bijective we know ϕ^{-1} exists and is bijective. Since ϕ^{-1} is bijective $\forall\, x, y \in G \,\exists!\, x', y' \in F$ such that $x' = \phi^{-1}(x)$ and $y' = \phi^{-1}(y)$. As ϕ is an homomorphism we have $\phi(x'y') = \phi(x')\phi(y')$ so $x'y' = \phi^{-1}(\phi(x')\phi(y'))$. Substituting for x' and y', $\phi^{-1}(x)\phi^{-1}(y) = \phi^{-1}(xy)$ immediately. □

2 The Symmetric and Dihedral Groups

Proposition 2.1. *$Sym(X)$ is a group under composition of functions.*

Proof. The elements of $Sym(X)$ are all bijections from X to itself. The compositions of two bijections from X to X is again a permutation of X. The identity function maps every element to itself. Since these maps are bijections their inverses exist. Also composition of functions is a associative. □

Lemma 2.2. *If $\sigma, \tau \in S_n$ are disjoint cycles then $\sigma \circ \tau = \tau \circ \sigma$, i.e. they commute.*

Proof. Let σ be represented in cycle notation by $(a_1, a_2, \cdots a_k)$ and τ by $(b_1, b_2, \cdots b_l)$ where $a_i \neq b_j \,\forall\, i, j$. Now take any element $x \in S_n$. If $x \notin \{a_i, b_j\}\; 1 \leq i \leq k, 1 \leq j \leq l$ Then $\sigma(\tau((x)) = x = \tau(\sigma(x))$. If $x = a_i$ for some $1 \leq i \leq k$ then $\sigma(\tau(a_i)) = \sigma(a_i) = a_{i+1} = \tau(a_{i+1}) = \tau(\sigma(a_i))$, where we take addition to be $mod\, k$. A similar argument works for if $x = b_j$ for some j. □

Theorem 2.3. *Every permutation in S_n can be written uniquely as a product of disjoint cycles (up to order).*

Proof. An inductive proof on n. If $n = 1$ there is only one permutation (1) this is a disjoint cycle. Assume that all permutations of a set of size $n < k$ can be written as the product of disjoint cycles. Now consider $\sigma \in S_k$, consider the sequence $1, \sigma(1), \sigma(1)^2, \sigma(1)^3, \cdots$. Now as S_k is finite there must be some repeating in this sequence, suppose $\sigma(1)^i = \sigma(1)^j$ where $i < j$ is the first repeated term of the sequence. But by taking the inverse σ of both sides i times we find that $\sigma(1)^{j-i} = 1$, this is the first repeating term. Let $m = j - i$. Consider the set $S = \{1, \sigma(1), \sigma(1)^2, \cdots \sigma(1)^{m-1}\}$, if $S = Q$ where $Q = \{1, 2, 3, \cdots k\}$ then we have a k-cycle and we are done. If $S \neq Q$ then $\sigma = (1, \sigma(1), \sigma(1)^2, \cdots \sigma(1)^{m-1})\tau$, where τ is a permutation of the set $S - Q = \{t \in S : t \notin Q\}$ Now as this set has an order smaller than k we can write it as a product of disjoint cycles say $\tau_1\tau_2 \cdots \tau_k$. So that $\sigma = (1, \sigma(1), \sigma(1)^2, \cdots \sigma(1)^{m-1})\tau_1\tau_2 \cdots \tau_k$, hence we have the required result for $n = k$ so by induction it holds for all n. To prove uniqueness we can prove that all cycles are disjoint or equal. To prove they are unique suppose $\sigma_1\sigma_2 \cdots \sigma_k = \sigma = \sigma_1^*\sigma_2^* \cdots \sigma_l^*$, if $\sigma_1(i) = j$ then there must be some p such that $\sigma_p^*(i) = j$ since the cycles are disjoint. Then consider $\sigma_1(j)$ by the same reasoning we $\sigma_1(j) = \sigma_p^*(j)$, inductively this shows $\sigma_1 = \sigma_p^*$ and we can cancel them. This process can continue to show the o factorisations are the same. □

Lemma 2.4. *Let $g \in G$. Then $g^n = e$ iff $o(g)|n$*

Proof. Let $m = o(g)$. Suppose $g^n = e$, then by Euclid's Algorithm this is equal to g^{qm+r} for some q and r with $0 \leq r \leq m$. Now $e = g^n = (g^m)^q g^r$ but $g^m = e$ so, $g^r = e$ but this means $r = 0$ by the minimality of m. So $o(g)$ must divide n. Now we prove the result the other way, suppose $n = qm$, then $g^n = g^{qm} = (g^m)^q = e$, hence if m divides divides n then the result holds, and we have shown the iff. □

Lemma 2.5. *Let $\sigma, \tau \in S_n$ be disjoint cycles in S_n. Then $o(\sigma\tau) = lcm(\sigma^*, \tau^*)$. ($\sigma^*$ is the length of σ, τ^* is similar).*

Proof. Consider $(\sigma\tau)^n = \sigma^n\tau^n$ because Lemma 2.2 tells us they commute. If n is the order of $\sigma\tau$ then n is the smallest positive integer such that for all $i \in \mathbb{Z}_n, (\sigma\tau)^n(i) = i$. This is true if and only if $\sigma^n = e$ and $\tau^n = e$. But then $\sigma^*|n$ and $\tau^*|n$, so the smallest such n is $lcm(\sigma^*, \tau^*)$. □

Proposition 2.6. *Any $\sigma \in S_n$ $(n \geq 2)$ can be written as a product of disjoint cycles.*

Proof. Let σ be expressed as the product of disjoint cycles, say $\sigma_1, \sigma_2, \cdots \sigma_r$. Take any of these cycles suppose it is represented in cycle notation by $(a_1, a_2, \cdots a_k)$, then we can express this as $(a_1a_2)(a_2a_3) \cdots (a_{k-1}a_k)$. The same holds for all σ_i so we can express σ as the product of transpositions. □

Lemma 2.7. *The function*

$$\begin{aligned} \text{sgn} : S_n &\longrightarrow \{\pm 1\} \\ \sigma &\longmapsto \text{sgn}(\sigma) \end{aligned}$$

is well defined.

Proof. First we show that the identity can be written as the product of an even number of permutations. Suppose the identity permutation on $\{1, 2, \cdots n\}$ is even. The base case $n = 2$ holds since $(12)^n = e$ iff n is even. Suppose the identity of the set $\{1, 2, \cdots n - 1\}$. Now consider $I = \tau_1\tau_2 \cdots \tau_m$ where each of the τ_i is a transposition acting on $\{1, 2, \cdots n\}$. $m \neq 1$, so $m \geq 2$. Suppose τ_m does not fix n, then we have for some a, b, c

$$\tau_{m-1}\tau_m = \begin{array}{ccccc} (nb)(na) & = & (abn) & = (na)(ab) \\ (ab)(na) & = & (anb) & = (nb)(ab) \\ (bc)(na) & = & (na)(bc) & \\ (na)(na) & = & I & = (ab)(ab) \end{array}$$

So we can write I where the first transposition fixes n. We can now continue this process until we have that $\tau_2, \tau_3, \cdots \tau_m$ fix n. But since we have the identity this mean τ_1 fixes n too. So we can write $I = \tau_1\tau_2 \cdots \tau_m$ which acts on $\{1, 2, \cdots n-1\}$, which by the induction hypothesis must be even. Now suppose that a permutation can be expressed in two different ways as the product of transpositions. If $\tau_1\tau_2 \cdots \tau_m = \tau = \tau_1^*\tau_2^* \cdots \tau_p^*$, then $I = \tau_1\tau_2 \cdots \tau_m\tau_p^*\tau_{p-1}^* \cdots \tau_1^*$, but we know this must have even length, so p and m are either both even or both odd.

□

Theorem 2.8. *Let $n \geq 2$. The map*

$$\begin{aligned} \operatorname{sgn} : (S_n, \circ) &\longrightarrow (\{\pm 1\}, \times) \\ \sigma &\longmapsto \operatorname{sgn}(\sigma) \end{aligned}$$

is a well defined, non-trivial homomorphism.

Proof. Lemma 2.7 shows it is well-defined. A transposition is mapped to -1, so the mapping is non-trivial. Suppose σ and τ are elements in S_n, if σ can be written as the product of m transpositions and τ can be written as the product of n then $\sigma\tau$ can be written as the product of $m+n$, so $sgn(\sigma\tau) = (-1)^{m+n} = (-1)^m(-1)^n = sgn(\sigma)sgn(\tau)$, so we have a homomorphism. □

Corollary 2.9. *The even permutations of S_n, $n \geq 2$, denoted A_n, form a subgroup of S_n.*

Proof. This follows from the first isomorphism theorem. □

3 Cosets and Lagrange

Lemma 3.1. *Let $H \leq G$ and $g \in G$. Then there is a bijection between H and gH. In particular, if H is finite, $|H| = |gH|$.*

Proof. Let $\psi : H \to gH$ such that $\psi(h) = gh$ where $h \in H$ and $g \in G$. If $gh_1 = gh_2 \Rightarrow h_1 = h_2$ by pre-multiplying by g^{-1}. So $\psi(h_1) = \psi(h_2) \Rightarrow h_1 = h_2$, so ψ is injective. Take any gh in gH, now $\exists\, h \in H$ such that $\psi(h) = gh$ so the mapping is surjective. (h are uniquely defined so there is no need to show the map is automatically well-defined.) □

Lemma 3.2. *Let $H \leq G$. The left cosets of H in G form a partition of G, i.e.*
(i) each $g \in G$ lies in some coset of H.
(ii) for $a, b \in G$, $aH \cap bH \neq \emptyset \Rightarrow aH = bH$.

Proof. (i) As $e \in H$, $g = ge \in gH$.
(ii) If $aH \cap bH \neq \emptyset$ then there exists $h_1, h_2 \in H$ such that $ah_1 = bh_2$. This means $a = bh_2h_1^{-1}$. So $aH = \{ah : h \in H\} = \{bh_2h_1^{-1}h : h \in H\} \subset bH$. The reverse inclusion follows by a similar argument so $aH = bH$. (The same holds for right cosets by a similar argument.) □

Lemma 3.3. *Let $H \leq G$ and $a, b \in G$. Then $aH = bH$ iff $a^{-1}b \in H$.*

Proof. If $aH = bH$ then $\exists\, h_1, h_2 \in H$ such that $ah_1 = bh_2$ so $a^{-1}b = h_1h_2^{-1} \in H$. If $a^{-1}b \in H$ then $a^{-1}b = h$ for some $h \in H$. So $a = bh^{-1} \in bH$ and as $a \in aH$, $aH \cap bH \neq \emptyset$, hence by Lemma 3.2 $aH = bH$. □

Theorem 3.4. *Lagrange's Theorem - Let H be a subgroup of a finite group G. Then the order of H divides the order of the group G.*

Proof. As G is finite we have a finite number of cosets. By Lemma 3.2 the cosets H of G form a partition of G. So G is the disjoint union of its cosets, $G = g_1H \cup g_2H \cup \cdots g_kH$. So $|G| = |g_1H| \cup |g_2H| \cup \cdots |g_kH|$. But by Lemma 3.1 every coset has the same size as $|H|$, so $|G| = k|H|$. $\frac{|G|}{|H|} = k$, so the order of H divides the order of G. □

Corollary 3.5. *Lagrange's corollary - Let G be a finite group and $g \in G$ then $o(g)|G$. In particular $g^{|G|} = e$.*

Proof. The element g (by composition with itself) produces the finite cyclic subgroup $\{e, g, g^2, \cdots g^{o(g)-1}\}$, this group has order $o(g)$. As this is a subgroup the result follows from Theorem 3.4. □

Corollary 3.6. *If $|G| = p$ for some prime p, then G is cyclic.*

Proof. As p is prime $p \geq 2$, so G has some non-identity element g. But by Lagrange's corollary the order of g must divide p. So $o(g)$ is 1 or p. Since $g \neq e$, g must have order p, so $\langle g \rangle = G$. So G is cyclic. □

Theorem 3.7. *(Fermat-Euler Theorem) - Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and $hcf(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 (\bmod n)$*

Proof. There is rather a lot to set up. Let $n \in \mathbb{N}$, define $R_n = \{0, 1, \cdots n-1\}$. And let $R_n^* = \{a \in R_n : hcf(a, n) = 1\}$, also $\times_n$ is multiplication modulo n.
We claim that $(R_n^*, \times_n)$ is a group. (Define $\bar{b}$ to be $b \in R_n$ such that $b \equiv \bar{b} \, (\bmod n)$) Suppose $a, b \in R_n^*$ then $hcf(a, n) = 1 = hcf(b, n) \Rightarrow hcf(ab, n) = 1$. So $hcf(\bar{ab}, n) = 1$, we have closure. The identity is 1. Let $a \in R_n^*$, so by Bezout there exists $u, v \in \mathbb{Z}$ such that $au + nv = 1$, so $\bar{u} \in R_n^*$ satisfies $\bar{u} = a^{-1}$. Multiplication modulo n is associative. Now we prove Fermat-Euler.
R_n^* is the group of all integers a coprime to n, so $|R_n^*| = \phi(n)$. Let $a \in \mathbb{Z}$, such that $hcf(a, n) = 1$, so $\bar{a} \in R_n^*$. By Lagrange $\bar{a}^{\phi(n)} = \bar{a}^{|R_n^*|} = 1$ in R_n^*. So $a^{\phi(n)} \equiv 1 \, (\bmod n)$. □

4 Normal Subgroups, Quotient Groups and Homomorphisms

Proposition 4.1. *Let $K \trianglelefteq G$. The following are equivalent,*
(i) $gK = Kg \; \forall g \in G$
(ii) $gKg^{-1} = K \; \forall g \in G$
(iii) $gkg^{-1} \in K \; \forall k \in K, g \in G$

Proof. Assume (i) holds then $gk = \hat{k}g$ for some $k, \hat{k} \in K$. So $gkg^{-1} = \hat{k} \in K$. This proves $(i) \Rightarrow (iii)$. If we now assume (iii), then $gKg^{-1} \subset K$. As this holds for all g we can replace g by g^{-1}, so we have $g^{-1}Kg \subset K$, which means $K \subset gKg^{-1}$. So $gKg^{-1} = K$. $(iii) \Rightarrow (ii)$. Finally, (i) is immediate from (ii) by right multiplication by g. □

Lemma 4.2. *If K is a subgroup of G of index two then K is normal in G.*

Proof. K has index 2, this means that K has two left cosets and two right cosets. One coset is always K itself. Take $g \notin K$. Then gK is the other left coset, Kg is the other right coset, and $K \cup gK = G = K \cup Kg$. But these are disjoint unions, so $gK = Kg$. By Lemma 4.2 this means that K is normal. □

Theorem 4.3. *If $K \trianglelefteq G$, the set $(G : K)$ of left cosets of K in G is a group, denoted $\frac{G}{K}$, under the operation coset multiplication i.e. $gK * hK = ghK$*

Proof. First we need to show coset multiplication is well defined. Namely if $a_1K = a_2K$ and $b_1K = b_2K$ then $a_1K * b_1K = a_2K * b_2K$. Now $a_1K * b_1K = a_1b_1K = a_1(b_2K) = (a_1K)b_2 = (a_2K)b_2 = a_2(Kb_2) = a_2b_2K$. Now if $a, b \in G$, then abK is a coset of K, so we have closure. $eK = K$ is the identity. Given aK, consider $aK * a^{-1}K = K = a^{-1}KaK$, so we have inverses. Finally, if $a, b, c \in G$, then $aK * (bK * cK) = aK * bcK = abcK = abK * cK = (aK * bK) * cK$ so associativity holds too. □

Theorem 4.4. *First Isomorphism Theorem - Let G, H be groups and $\theta : G \to H$ a group homomorphism. Then,*
(i) $Im(\theta) \leq H$
(ii) $Ker(\theta) \trianglelefteq G$
(iii) $\frac{G}{ker\theta} \cong Im(\theta)$

Proof. (i) Let $Im(x), Im(y) \in Im(\theta)$. $\theta(x)\theta(y) = \theta(xy) \in Im(\theta)$. The identity of H is in $Im(\theta)$ since $\theta(e_G) = e_H$. Let $\theta(x') \in Im(\theta)$, consider $\theta(x')\theta((x')^{-1}) = \theta(x'(x')^{-1}) = \theta(e_G) = e_H$, so inverses exist. Associativity holds due to the homomorphism.
(ii) Take two elements $x, y \in Ker(\theta)$, consider $\theta(xy) = \theta(x)\theta(y) = e_H$. So $xy \in Ker(\theta)$. The identity is e_G. Take any $x \in Ker(\theta)$, consider $xx^{-1} = e_G$, but $\theta(x^{-1}) = (\theta(x))^{-1} = e_H$. So $x^{-1} \in Ker(\theta)$. G is associative so associativity is inherent in $Ker(\theta)$. Now take any $g \in G$, consider $\theta(gkg^{-1})$ where $k \in Ker(\theta)$. $\theta(gkg^{-1}) = \theta(g)\theta(k)\theta(g^{-1}) = \theta(g)(\theta(g))^{-1} = e_H$. So $gkg^{-1} \in Ker(\theta), \forall g \in G, k \in Ker(\theta)$. So the kernel is a normal subgroup.
(iii) Define $\varphi : G \backslash Ker(\theta) \to \theta(G)$ by $\varphi(gKer(\theta)) = \theta(g)$. We need to show this map is well-defined, a homomorphism, injective and surjective.
Well-defined - Suppose $aKer(\theta) = bKer(\theta)$, then $a = bk$ for some $k \in Ker(\theta)$. Now $\varphi(aKer(\theta)) = \theta(a) = \theta(bk) = \theta(b) = \varphi(bKer(\theta))$, so the map is well-defined.
Homomorphism - $\varphi(aKer(\theta))\varphi(bKer(\theta)) = \theta(a)\theta(b) = \theta(ab) = \varphi(abKer(\theta))$.
Injective - If $\varphi(aKer(\theta)) = \varphi(bKer(\theta))$ then $\theta(a) = \theta(b)$. Consider $\theta(ab^{-1}) = \theta(a)(\theta(b))^{-1} = e_H$, so $ab^{-1} \in Ker(\theta)$, hence $aKer(\theta) = bKer(\theta)$ by Lemma 3.3. So $\varphi(aKer(\theta)) = \varphi(bKer(\theta)) \Rightarrow aKer(\theta) = bKer(\theta)$. so φ is injective.
Surjective - Take any element $x \in Im(\theta)$, then there exists $g \in G$ such that $\theta(g) = x$. But then $\varphi(gKer(\theta)) = \theta(g) = x$. So φ is surjective. $\square$

Lemma 4.5. *A homomorphism $\theta : G \to H$ is injective iff $Ker(\theta) = \{e_G\}$.*

Proof. If θ is injective then $\theta(x) = y$ for at most one $x \in G$, which immediately shows $Ker(\theta) = \{e_G\}$. If $Ker(\theta) = \{e_G\}$ then consider $\theta(x) = \theta(y) \Rightarrow \theta(x)\theta(x^{-1}) = \theta(y)\theta(x^{-1}) \Rightarrow \theta(e_G) = \theta(xy^{-1})$ but $Ker(\theta) = \{e_G\}$ so $xy^{-1} = e \Rightarrow x = y$ so θ is injective. $\square$

Lemma 4.6. *(i) Let $N \trianglelefteq G$ and $H \leq G$, then $NH \leq G$*
(ii) Let $N \trianglelefteq G$ and $M \trianglelefteq G$, then $NM \trianglelefteq G$

Proof. (i) First, since all $n \in N, h \in H$ are in G, this means all $nh \in N \in G$. Now take $n_1h_1, n_2h_2 \in NH$, consider $n_1h_1n_2h_2$, as N is normal $h_1N = Nh_1$ so $h_1n_1 = \hat{n}h_1$ for some $\hat{n} \in N$. So $n_1\hat{n}h_1h_2 \in NH$. The identity is still $e_Ge_G = e_G$. Associativity is inherent since G is a group. Now take any $nh \in NH$, select the element $(h^{-1}n^{-1}h)h^{-1}$. $h^{-1}n^{-1}h$ is an element of G of the form ghg^{-1} so we can be sure it's in N (so $(h^{-1}n^{-1}h)h^{-1} \in NH$) Now $nh(h^{-1}n^{-1}h)h^{-1} = e_G$, so we have inverses.
(ii) Part (i) immediately tells us $NM \leq G$. Let $n \in N, m \in M, g \in G$, consider $gnmg^{-1}$. Since N normal $gN = Ng$ so $gn = \hat{n}g$ for some $\hat{n} \in N$. Similarly, $gm = \hat{m}g$ for some $\hat{m} \in M$. So $gmn^{-1} = \hat{m}gng^{-1} = \hat{m}\hat{n}gg^{-1} = \hat{m}\hat{n} \in MN$. This holds for all $g \in G$, so MN is normal in G. $\square$

5 Direct Products and Small Groups

Lemma 5.1. *Let $(h,k) \in H \times K$, then $o((h,k)) = (o(h), o(k))$.*

Proof. Consider raising (h,k) to the power n. $(h,k)^n = (h^n, k^n)$. Now $o((h,k))$ is the smallest integer n such that $(h^n, k^n) = (e_H, e_K) \Leftrightarrow h^n = e_H$ and $k^n = e_K$, the smallest such n is $lcm(o(h), o(k))$ $\square$

Corollary 5.2. *$C_m \times C_n \cong C_{mn}$ iff $hcf(m,n) = 1$.*

Proof. First note $|C_m \times C_n| = mn$. Now $C_m \times C_n \cong C_m \times C_n \Leftrightarrow C_m \times C_n$ contains an element of order $mn \Leftrightarrow lcm(m,n) = 1 \Leftrightarrow hcf(m,n) = 1$. $\square$

Proposition 5.3. *Let G be a group with subgroups H and K. If*
(i) each element of G can be written as hk with $h \in H$ and $k \in K$
(ii) $H \cap K = \{e\}$
(iii) $hk = kh \forall h \in H, k \in K$
then $G \cong H \times K$ and we call G the internal direct product of H and K.

Proof. Define the map $\varphi : H \times K \to G$ by $\varphi((h, k)) = hk$. If we can show this is an isomorphism we are done. Suppose $h_1 k_1 = h_2 k_2$ then $h_2^{-1} h_1 = k_2 k_1^{-1} = e$ by (ii). So we have $h_1 = h_2$ and $k_1 = k_2$. So $\varphi(h_1, k_1) = \varphi(h_2, k_2) \Rightarrow (h_1, k_1) = (h_2, k_2)$, φ is injective. Take any $g \in G$, by (i) we know there is $(h, k) \in H \times K$ such that $\varphi((h, k)) = g$, φ is surjective. Now consider (using (iii)) $\varphi(h_1 k_1 h_2 k_2) = \varphi(h_1 h_2 k_1 k_2) = (h_1 h_2, k_1 k_2) = (h_1, k_1)(h_2, k_2) = \varphi((h_1, k_1))\varphi((h_2, k_2))$, so φ is a homomorphism. ☐

6 Group Actions

Lemma 6.1. *Suppose G acts on the non-empty set X. Fix $g \in G$, then the map $\phi_g : X \to X$ such that $x \to \rho(g, x)$ is a permutation.*

Proof. By the definition of the map X is mapped to X. Now take ϕ_g, consider $\phi_{g^{-1}}(\phi_g(x)) = \phi_{gg^{-1}}(x) = e(x) = x$. So an inverse map exists so ϕ_g must be bijective, this defines a permutation of X. (So $\phi_g \in Sym(X)$) ☐

Proposition 6.2. *Suppose G acts on the set X. Then the map $\varphi : G \to Sym(X)$ such that $g \to \phi_g$ (where ϕ_g is as in Lemma 6.2) is a homomorphism.*

Proof. Take any $g_1, g_2 \in G$ and any $x \in X$, then $\varphi(g_1 g_2)(x) = \phi_{g_1 g_2}(x) = (g_1 g_2)(x) = g_1(g_2(x)) = \phi_{g_1}(\phi_{g_2}(x)) = \varphi(g_1)\varphi(g_2)(x)$. I'm unsure of the validity of this one, please advise me. ☐

Theorem 6.3. *(Cayley's Theorem) - Any group G is isomorphic to a subgroup of $Sym(X)$ for some set X.*

Proof. Let G act on the set $X = G$, with G acting by left multiplication. (This is the left regular action.) This is an action because (for any $x \in X$ and $g_1, g_2 \in G$) $ex = x$ and $g_1 g_2 x = (g_1 g_2)x$. Since G acts we have a homomorphism $\varphi : G \to Sym(G)$. Now if $g_1 x = g_2 x \Rightarrow g_1 = g_2$, so the homomorphism is injective. So $G \cong Im(\varphi) \leq Sym(G)$. ☐

Lemma 6.4. *The distinct orbits form a partition of X.*

Proof. Let the group G act on the set X. Every element $x \in X$ is in at least one orbit since $e(x) = x$. Now suppose two orbits, $Orb(x)$ and $Orb(y)$ have a common element z, then $g_1 x = z$ and $g_2 y = z$ for some $g_1, g_2 \in G$. Now take any point $u \in Orb(x)$, $u = gx = gg_1^{-1} z = (gg_1^{-1})g_2 = (gg_1^{-1} g_2)y$ so $\forall u \in Orb(x) \subset Orb(y)$. The reverse inclusion holds by a similar argument. So $Orb(x) = Orb(y)$, orbits are distinct or equal. ☐

Lemma 6.5. *$Stab_G(x)$ is a subgroup of G.*

Proof. Since $e(x) = x$, $e \in Stab_G(x)$. Now if $g_1, g_2 \in G$ then $(g_1 g_2)(x) = g_1(g_2(x)) = g_1(x) = x$, so we have closure. Take any $g \in G$, then consider $g^{-1}(g(x)) = (g^{-1}g)(x) = e(x)$, so we have inverses. As G is a group associativity is inherent. ☐

Theorem 6.6. *(Orbit-Stabiliser Theorem) - Let G be a finite group acting on a set X. Let $x \in X$, then $|G| = |Stab_G(x)||Orb_G(x)|$.*

Proof. Let $(G : Stab_G(x))$ be the set of left cosets of $Stab_G(x)$ in G. Let $\varphi : Orb_G(x) \to (G : Stab_G(x))$ such that $g(x) \to gStab_G(x)$. Suppose $g_1(x) = g_2(x) \Leftrightarrow g_2^{-1} g_1(x) = x \Leftrightarrow g_2^{-1} g_1 \in Stab_G(x) \Leftrightarrow g_1 Stab_G(x) = g_2 Stab_G(x)$, so the map is well defined and injective. Now take any $gStab_G(x) \in (G : Stab_G(x))$, $\varphi(g(x)) = gStab_G(x)$ so we have a surjective map, hence φ is a well-defined bijection. ☐

Theorem 6.7. *(Cauchy's Theorem) - Let G be a finite group and p be a prime with p divides $|G|$. Then there exists an element in G of order p.*

Proof. We are looking for non-trivial solutions to the equation $g^p = 1$, McKay's idea is to look at a more general equation. Namely, let $X = \{(x_1, x_2, \cdots x_p : x_1 x_2) \cdots x_p = e\}$ with all the $x_i \in G$. Let the cyclic group C_p ($\langle a \rangle$) act on X, so that $a^k(x_1, x_2, \cdots x_p) = (x_{1+k}, x_{2+k}, \cdots x_{p+k})$ where addition is $\pmod p$. This is an action. $|X| = |G|^{p-1}$ since x_p is predetermined by the $p-1$ (independent) previous terms. By the orbit-stabiliser theorem the orbits of elements in X is 1 or p. Orbits of size 1 correspond to elements of X of the form $x^p = e$, we know we have at least one since $e^p = e$ is trivially a solution. But as $|X| = |G|^{p-1}$ (and p divides $|G|$), $|X| \equiv 0 \pmod p$. So there must at least $p-1$ other elements that satisfy $x^p = e$, (and hence $g^p = e$). ☐

Proposition 6.8. *Let p be a prime and G a group of order p^n, for some $n \geq 1\,(n \in \mathbb{N})$. Then the centre $Z(G)$ is non-trivial. I.e. $|Z(G)| \geq |\{e\}|$.*

Proof. If $a \in G$ is in the centre then $ga = ag \;\forall\, g \in G$. This can also be written as $gag^{-1} = a$. Let G act on itself ($X = G$) by conjugation. So $g(x) = gxg^{-1}$. Consider orbits of $x \in X$, by the orbit-stabiliser theorem (and Lagrange) we know orbits must be of size $1, p, p^2, \cdots p^n$. We know $|G| \equiv 0 \pmod p$, but if we look at G as the union of its disjoint orbits (we know we have one of size 1 namely $\{e\}$), this means there must be at least $p-1$ other orbits of size 1. Orbits of size 1 correspond to elements of the centre (since if $gag^{-1} = a \;\forall\, g \in G$ the orbit of a is just $\{a\}$). ☐

Lemma 6.9. *Let G be a finite group and $Z(G)$ be the centre of G. If $G \backslash Z(G)$ is cyclic then G is abelian.*

Proof. First note the centre is a normal subgroup so the set of left cosets of $Z(G)$ in G is a group. As $G \backslash Z(G)$ is cyclic every coset can be written in the form $a^i Z(G)$ for some $a \in G$, where $0 \leq i \leq k-1$ ($k = |G|/|Z(G)|$). So every element in G is of the form $a^i c$, where $c \in Z(G)$. Now let G act on itself by conjugation. Consider the action of $a^i c_1$ on $a^j c_2$ ($a^i, a^j \in G, c_1, c_2 \in Z(G)$), we have $a^i c_1(a^j c_2) = a^i c_2 a^j c_1 a^{k-i} {c_2}^{-1} = a^i a^j a^{k-i} c_2 c_1 c_2^{-1} = a^j c_2 {c_2}^{-1} c_1 = a^j c_2$. So the orbit of any $g \in G$ contains only g. But this means every element is in the centre, so the group is abelian. ☐

Corollary 6.10. *Suppose $|G| = p^2$ for some prime p. Then G is abelian and, up to isomorphism there are only two groups of order p^2, namely C_{p^2} and $C_p \times C_p$.*

Proof. From proposition 6.8, we know the centre of G is non-trivial. So $|Z(G)| = p$ or p^2.
First consider if $|Z(G)| = p$, $G \backslash Z(G)$ has order p, so it must be isomorphic to C_p. From Lemma 6.9 we know G group must be abelian. By Lagrange G contains two elements of order p. Let these be b, c with $b \neq c$ (let the corresponding subgroups be B, C, with $B \neq C$). Suppose $\langle b \rangle \cap \langle c \rangle \neq \{e\}$, then $b^i = c^k$ for some $1 \leq i, k \leq p-1$, but this element generates both B and C which is a contradiction. All conditions of proposition 5.3 are met so we see $G \cong C_p \times C_p$.
Now consider if $|Z(G)| = p^2$, $G \backslash Z(G)$ is trivial (cyclic) so G is abelian. G contains an element of order p^2 so it must be the cyclic group C_{p^2}. ☐

Theorem 6.11. *The permutations π and σ in S_n are conjugate in S_n iff they are of the same cycle type.*

Proof. If π and σ are conjugate then there exists some element $\tau \in S_n$ such that $\sigma = \tau\pi\tau^{-1}$. Let $\pi(i) = j$, σ is simply a relabelling of π because $(\tau\pi\tau^{-1})(\tau(i)) = \tau\pi(i) = \tau(j)$ $(*)$. So σ is τ with every element x in τ relabelled as $\tau(x)$. So they have the same cycle type. Given two permutations π and σ in S_n of the same cycle type, we can show they are conjugate as follows, list the cycles of π above the cycles of σ, aligning cycles of the same length with one another. Now interpret this as the two-line presentation of a permutation, and call it τ then $\tau\pi\tau^{-1} = \sigma$ by $(*)$. ☐

Corollary 6.12. *The number of distinct conjugacy classes in S_n is given by $p(n)$, the number of partitions of n into positive integers i.e. $n = n_1 + n_2 + \cdots n_k$ with $n_1 \geq n_2 \geq \cdots n_k \geq 1$.*

Proof. From Theorem 6.11 we see that the conjugacy classes of S_n are the cycle types. Each cycle type corresponds to a partition of n. So the number of cycle types is the number of partitions and the result holds. ☐

Cycle Type (Conjugacy Class)	Size	Sign
e	1	+
2	10	-
2,2	15	+
2,3	20	-
3	20	+
4	30	-
5	24	+

Theorem 6.13. *A_5 is a simple group.*

Proof. Conjugacy classes split moving from S_5 to A_5 iff they have a cycle type consisting of odd and distinct length cycles. First consider the conjugacy classes of S_5 (these are by Theorem 6.11 just the cycle types). Only the even permutations appear in A_5, by the above rule the only conjugacy class that will split is 5-cycles. So in A_5 we have conjugacy classes of size $1, 12, 12, 15, 20$. A subgroup is normal iff it is the union of some conjugacy classes (it must include $\{e\}$ too). But the union of $\{e\}$ and any combination of the other conjugacy classes is never a divisor of 60, so we cannot (by Lagrange) have a subgroup. So A_5 has no normal subgroups other than the trivial and improper subgroups hence it is simple. □

7 Matrix Groups

Proposition 7.1. *$GL_n(\mathbb{R})$ is a group under matrix multiplication.*

Proof. Take any two matrices $A, B \in GL_n(\mathbb{R})$, $AB \in GL_n(\mathbb{R})$ since as $\det(A)\det(B) = \det(AB) \Rightarrow \det(AB) \neq 0$. The identity is I. Multiplication of matrices is associative. Finally, as the members of $GL_n(\mathbb{R})$ have non-zero determinants their inverses exist. □

Proposition 7.2. *The map $Det : GL_n(\mathbb{R}) \to (\mathbb{R}\backslash\{0\}, \times)$, such that $A \to \det A$, is a surjective homomorphism.*

Proof. Take any $A, B \in GL_n(\mathbb{R})$, the determinant property $\det(A)\det(B) = \det(AB)$ immediately tells us we have a homomorphism. Take any $x \in \mathbb{R}\backslash\{0\}$, consider the matrix A with entries $a_{11} = x, a_{ii} = 1$ $(2 \leq i \leq n)$, and $a_{ij} = 0$ where $i = j$, this matrix is in $GL_n(\mathbb{R})$ and has $\det(A) = x$, so the map is surjective. □

Proposition 7.3. *$O_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.*

Proof. $O_n(\mathbb{R})$ are the set of n by n orthogonal matrices. Orthogonal matrices have determinant ± 1 so $O_n(\mathbb{R}) \subset GL_n(\mathbb{R})$. Take any two $A, B \in O_n(\mathbb{R})$, consider $AB(AB)^T = ABB^TA^T = AA^T = I$, so $AB \in O_n(\mathbb{R})$. The identity matrix is orthogonal. The inverse of an orthogonal matrix A is A^T, which is also orthogonal. Finally, associativity is inherent. □

Lemma 7.4. *Let $\mathbf{A} \in O_n(\mathbb{R})$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$*
(i) $\mathbf{Ax} \cdot \mathbf{Ay} = \mathbf{x} \cdot \mathbf{y}$
(ii) $|\mathbf{Ax}| = |\mathbf{x}|$

Proof. To me this becomes more obvious in suffix notation. Let A have entries a_{ij}, then $Ax \cdot Ay = \sum_i x'_i y'_i$ where $x'_i = \sum_j a_{ij}x_j$ and $y'_i = \sum_k a_{ik}y_k$. So using the summation convention we have $Ax \cdot Ay = a_{ij}x_j a_{ik}y_k = a_{ij}a_{ik}x_jy_k$, but $a_{ij}a_{ik}$ is $AA^T = I$, so $Ax \cdot Ay = \delta_{jk}x_jy_k = x_jy_j$ which is the scalar product of x and y.
(ii) follows from (i) with $x = y$. □

Proposition 7.5. *Let $\mathbf{A} \in SO_3(\mathbb{R})$. Then $\mathbf{A}$ has an eigenvector with corresponding eigenvalue 1.*

Proof. A has an eigenvector because every square matrix does. Now consider $\det(A-I) = \det(A^T)\det(A-I) = \det(I - A^T) = -\det(A^T - I) = -\det((A-I)^T) = -\det(A-I)$. So $\det(A-I) = 0$ so A has a eigenvalue of 1. □

Theorem 7.6. *Let $\mathbf{A} \in SO_3(\mathbb{R})$. Then $\mathbf{A}$ is conjugate to a matrix of the form*

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for some $\theta \in [0, 2\pi)$. In particular, $\mathbf{A}$ is a rotation about an axis through the origin.

Proof. By proposition 7.5 there exists $\vec{v}$ which is an eigenvector of A with eigenvector 1. Let $\{e_1, e_2, e_3\}$ be the standard orthonormal basis of $\mathbb{R}^3$. There is some $P \in SO_3(\mathbb{R})$ such that $P\vec{v} = e_3$. Now, $PAP^{-1}(e_3) = e_3$, and if Π is the plane orthogonal to e_3 ($\Pi = \langle e_1, e_2 \rangle$), then $PAP^{-1} : \Pi \to \Pi$. So

$$PAP^{-1} = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the action on Π. But we know $PAP^{-1} \in SO_3(\mathbb{R})$ so $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$. Also (a, c) and (b, d) must be an orthonormal basis for Π hence $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^T = I$. Which means $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. □

Theorem 7.7. *Any element of $O_3(\mathbb{R})$ is a product of at most 3 reflections.*

Proof. Let $f(x) = Ax$ with $A \in O_3(\mathbb{R})$ and let e_1, e_2, e_3 be the standard orthonormal basis for $\mathbb{R}^3$. Now A is an isometry so $|f(e_3) - f(0)| = |e_3 - 0| \Rightarrow |f(e_3)| = |e_3|$. So there is a reflection r_1 in a plane through the origin with $r_1 f(e_3) = e_3$. $r_1 f$ maps the plane Π generated by e_1, e_2 onto itself. Now, there is a reflection r_2 with $r_2(e_3) = e_3$ and $r_2 r_1 f(e_2) = e_2$. So $r_2 r_1 f : e_3 \mapsto e_3, e_2 \mapsto e_2$, so $e_1 \mapsto \pm e_1$. Let r_3 be a reflection in a plane normal e_1 if $r_2 r_1 f(e_1) = -1$ and the identity map otherwise. $r_3 r_2 r_1 f = I \Rightarrow f = r_1 r_2 r_3$. □

Proposition 7.8. *Suppose there exists at least 3 values of z in $\mathbb{C}$ such that*

$$\frac{az + b}{cz + d} = \frac{\alpha z + \beta}{\gamma z + \delta} \quad (*)$$

$ad - bc \neq 0$, $\alpha\delta - \beta\gamma \neq 0$. Then there exists $\lambda \neq 0$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

i.e. the two maps agree on all of $\mathbb{C}_\infty$.

Proof. If we multiply through by the denominators in $(*)$ we get $(az + b)(\gamma z + \delta) = (\alpha z + \beta)(cz + d)$. But since this equality holds for at least 3 values of z then it must be identically equal for all z, so we can compare coefficients. Hence, $a\gamma = \alpha c$, $b\gamma + \delta a = \beta c + \alpha d$ and $b\delta = \beta d$. This is equivalent to,

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix}$$

with μ not equal to zero (both determinants on LHS $\neq 0$), inverting the left most matrix we get,

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \frac{\mu}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

, which is the required form. □

Theorem 7.9. *The set $\mathcal{M}$ of all Möbius maps on $\mathbb{C}_\infty$ is a group under composition. It is a subgroup of* $\mathrm{Sym}(\mathbb{C}_\infty)$.

Proof. Take any two Möbius maps

$$f(z) = \frac{az+b}{cz+d} \text{ and } g(z) = \frac{\alpha z+\beta}{\gamma z+\delta}$$

$$f(g(z)) = \frac{(a\alpha+b\gamma)z+(a\beta+b\delta)}{(c\alpha+d\gamma)z+(c\beta+d\delta)}$$

Now consider determinants $(c\beta+d\delta)(a\alpha+b\gamma)-(a\beta+b\delta)(c\alpha+d\gamma) = (ad-bc)(\alpha\beta-\gamma\delta) \neq 0$ so this is a Möbius map. There are special cases but they are tedious. The identity map is $\frac{z+0}{0z+1}$. Composition of functions is associative. The inverse of f is $f^*(z) = \frac{dz-b}{-cz+a}$, but we need to carefully verify this. If $z \neq -d/c, \infty$, then

$$f^*f(z) = \frac{(ad-bc)z}{ad-bc} = z \ \text{ (since } ad-bc \neq 0)$$

And if $z \neq -a/c, \infty$ then $ff^*(z) = z$. Now $f^*f(-d/c) = f^*(\infty) = -d/c$ and $f^*f(\infty) = f^*(a/c) = \infty$, so as f has an inverse it bijects $\mathbb{C}_\infty$ onto itself, hence $\mathcal{M}$ is a subgroup of $Sym(\mathbb{C}_\infty)$. ☐

Theorem 7.10. $(GL_2(\mathbb{C}))\backslash Z \cong \mathcal{M}$ *where* $Z = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in GL_2(\mathbb{C}),\ \lambda \neq 0 \right\}$.

Proof. Consider the map $\varphi : GL_2(\mathbb{C}) \to \mathcal{M}$ defined by

$$\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \frac{az+b}{cz+d}$$

This is a homomorphism because

$$\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\varphi\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right).$$

The second equality comes from when we proved closure in Theorem 7.9. The kernel of this homomorphism is precisely Z. So by the first isomorphism theorem the result follows. ☐

Corollary 7.11. $\frac{SL_2(\mathbb{C})}{\{\pm \mathbf{I}\}} \cong \mathcal{M}$.

Proof. $SL_2(\mathbb{C}) \leq GL_2(\mathbb{C})$, where every member of $SL_2(\mathbb{C})$ has determinant 1. The map $\varphi : SL_2(\mathbb{C}) \to \mathcal{M}$, is still a homomorphism because $SL_2(\mathbb{C})$ is a subgroup (I believe this is correct, please anyone correct me if I am wrong.) The kernel this times is $\{\pm I\}$, so the result follows. ☐

Proposition 7.12. *Every Möbius map can be written as a composition of maps of the following forms:*
(i) $f(z) = az$; $a \neq 0$ *dilation or rotation*
(ii) $f(z) = z+b$; *translation*
(iii) $f(z) = \frac{1}{z}$; *inversion.*

Proof. First, if $c = 0$ then $f(z) = (a/d)z + b/d$ so $f = f_2f_1$ where $f_1(z) = (a/d)z$ and $f_2(z) = z + b/d$. If $c \neq 0$ then $f = f_4f_3f_2f_1$ where $f_1(z) = z + d/c$, $f_2(z) = 1/z$, $f_3(z) = -\frac{ad-bc}{c^2}z$ and $f_4(z) = z + a/c$. ☐

Theorem 7.13. *The action of* $\mathcal{M}$ *on* $\mathbb{C}_\infty$ *is sharply triply transitive.*

Proof. Given z_1, z_2, z_3 and w_1, w_2, w_3, we need to show there is a unique Möbius map, f, such that $f(z_i) = w_i$. First suppose none of the $z_i = \infty$. Then the map g

$$g(z) = \frac{(z_2-z_3)(z-z_1)}{(z_2-z_1)(z-z_3)}$$

maps z_1 to 0, z_2 to 1 and z_3 to ∞. If one of the $z_i = \infty$. Then take some $z_4 \neq z_i$ for $i = 1, 2, 3$. Let $g' = 1/(z-z_4)$, so g' maps the z_i to $g'(z_i)$ where none of the $g'(z_i)$ are infinite. The we can construct a map

g^* that takes $g'(z_1)$ to 0, $g'(z_2)$ to 1 and $g'(z_3)$ to ∞. So g^*g' (our new g) takes z_1 to 0, z_2 to 1 and z_3 to ∞. In a similar manner we can construct a map h such that $h(w_1) = 0, h(w_2) = 1, h(w_3) = \infty$. Then $f = g^{-1}h$ is our required map. Now we need a mini-lemma, if a Möbius map fixes three points then it must be the indetity map. Taking the standard Möbius map we see that $z(cz+d) = az+b$, for 3 values of z, so $z(cz+d) \equiv az+b$, which means $c = 0, a = d$ and $b = 0$, this defines the identity map. Now suppose there are two maps f, f' with $f(z_i) = w_i$ and $f'(z_i) = w_i$. Then Then ff'^{-1} fixes the three z_i so $ff'^{-1} = I$, which means $f = f'$. ☐

Theorem 7.14. *Any non-identity Möbius map is conjugate to one of*
(i) $f(z) = \nu z,\ \nu \neq 0, 1$
(ii) $f(z) = z + 1$

Proof. Consider first the conjugacy classes of $GL_2(\mathbb{R})$, these are the matrices

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} : \lambda \neq \mu, \lambda \neq 0 \neq \mu \text{ and } \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

Now let φ be as in Theorem 7.1 let A and B be conjugate in $GL_2(\mathbb{R})$, so there is $P \in GL_2(\mathbb{R})$ such that $PAP^{-1} = B \Rightarrow \varphi(P)\varphi(A)\varphi(P)^{-1} = \varphi(B)$, so the corresponding Möbius maps are conjugate too. Now $\varphi((\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix})) = z \mapsto z$, $\varphi((\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix})) = z \mapsto \nu z$ where $\nu \neq 0, 1$, finally $\varphi((\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix})) = z \mapsto z + \lambda^{-1}$. Now, every matrix that is conjugate to $(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix})$ is also conjugate to $(\begin{smallmatrix} 1 & \lambda^{-1} \\ 0 & 1 \end{smallmatrix})$ (since for any scalar β, $(\beta P)A(\beta P)^{-1} = \beta PA\beta^{-1}P^{-1} = PAP^{-1} = B$). But $(\begin{smallmatrix} 1 & \lambda^{-1} \\ 0 & 1 \end{smallmatrix})$ is conjugate to $(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$, since $(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix})(\begin{smallmatrix} 1 & \lambda^{-1} \\ 0 & 1 \end{smallmatrix})(\begin{smallmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{smallmatrix}) = (\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$. So $z \mapsto z + \lambda^{-1}$ is conjugate to $z \mapsto z + 1$. From this every non-identity Möbius map must be conjugate to $f(z) = \nu z,\ \nu \neq 0, 1$, or $g(z) = z + 1$ ☐

Corollary 7.15. *A non-identity Möbius map f has either*
(i) two fixed points $(0$ *and* $\infty)$ *or*
(ii) one fixed point (∞)

Proof. Suppose gfg^{-1}, then α is a fixed point of f iff $g(\alpha)$ is a fixed point of h. So the number of fixed points of f is equal to the number of fixed points of h. By Theorem 7.14, if f conjugate to $z \mapsto \nu z$ then since this has two fixed points $0, \infty$, so must f. If f is conjugate to $z \mapsto z + 1$ then ∞ is the only fixed point. ☐

Theorem 7.16. *Let $f \in \mathcal{M}$ and C a circle or line in $\mathbb{C}_\infty$, then $f(C)$ is a circle or line in $\mathbb{C}_\infty$.*

Proof. The general equation for a line or a circle in $\mathbb{C}$ is $az\bar{z} + b\bar{z} + \bar{b}z + c = 0$ (with $a = 0$ a line). But in $\mathbb{C}_\infty$ Cartesian lines are 'circles' which include the point at ∞. Now every Möbius is a composition of simpler maps by proposition 7.12, so we can consider each of these individually. For $f(z) = az$ and $f(z) = z + b$, both map Cartesian circles to Cartesian lines and Cartesian lines to Cartsian lines (with $g(\infty), f(\infty) = \infty$), so the result holds for these. Now consider $h(z) = 1/z$, let $w = 1/z$, so the equation of the line or circle becomes $cw\bar{w} + \bar{b}\bar{w} + bw + a = 0$. Which is again of the form of a line or a circle. Finally need to consider special cases. Suppose C passed through the origin, $C = \{z\,(z \neq 0) : az\bar{z} + b\bar{z} + \bar{b}z = 0\} \cup \{0\}$, we apply $f(z) = 1/z$ separately to get $f(C) = \{\bar{b}\bar{w} + bw + a = 0\} \cup \{\infty\}$ which is an extended line. In a similar way extended lines are mapped to Cartesian circles if they don't pass through the origin and extended lines if they do. ☐

Theorem 7.17. *Given $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ all distinct and $w_1, w_2, w_3, w_4 \in \mathbb{C}_\infty$ all distinct, then $\exists\, f \in \mathcal{M}$ such that $f(z_i) = w_i$ iff $[z_1, z_2, z_3, z_4] = [w_1, w_2, w_3, w_4]$. In particular, Möbius maps preserve cross ratios (i.e. $[z_1, z_2, z_3, z_4] = [f(z_1), f(z_2), f(z_3), f(z_4)]$).*

Proof. First suppose there is a Möbius map f such that that $f(z_i) = w_i$, with all $z_i, w_i \neq \infty$. Then for any j and k (with none of the terms in the fraction being zero or infinity where $j \neq k$)

$$w_j - w_k = f(z_j) - f(w_k) = \frac{(ad - bc)(z_j - z_k)}{(cz_j + d)(cz_k + d)}$$

Hence

$$\frac{(w_1 - w_3)(w_2 - w_4)}{(w_1 - w_3)(w_2 - w_4)} = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_3)(z_2 - z_4)}$$

which means $[z_1, z_2, z_3, z_4] = [w_1, w_2, w_3, w_4]$. If any of the $z_i, w_i = \infty$ then the formula for the cross-ratio can be adapted suitably with limits and the result still holds. Now suppose we have $[z_1, z_2, z_3, z_4] = [w_1, w_2, w_3, w_4]$ and let g and h be the Möbius maps such that $g(z_1) = 0$, $g(z_2) = 0$, $g(z_4) = \infty$ and $h(w_1) = 0$, $h(w_2) = 1$, $h(w_4) = \infty$. Now consider $g(z_3) = [0, 1, g(z_3), \infty] = [g(z_1), g(z_2), g(z_3), g(z_4)] = [z_1, z_2, z_3, z_4] = [w_1, w_2, w_3, w_4] = [h(w_1), h(w_2), h(w_3), h(w_4)] = [0, 1, h(w_3), \infty] = h(w_3)$. Let $f = h^{-1}g$ so that $f(z_i) = w_i$. $\square$

Corollary 7.18. *z_1, z_2, z_3, z_4 lie in some circle or line in $\mathbb{C}_\infty$ iff $[z_1, z_2, z_3, z_4] \in \mathbb{R}$.*

Proof. Let z_1, z_2, z_4 lie on some line or circle $C \in \mathbb{C}_\infty$. If g is the Möbius map such that $g(z_1) = 0$, $g(z_2) = 1$ and $g(z_4) = \infty$, then $f(C) = \mathbb{R} \cup \infty$ (the circle of the real axis and ∞). But

$$[z_1, z_2, z_3, z_4] = [g(z_1), g(z_2), g(z_3), g(z_4)] = [0, 1, g(z_3), \infty] = g(z_3)$$

so $[z_1, z_2, z_3, z_4] \in \mathbb{R}$ iff $g(z_3) \in \mathbb{R}$, which is true iff $z_3 \in C$. $\square$