Groups

Propositions, Lemmas, Theorems and Corollaries

Lectured by Dr Rachel Camina

Michaelmas 2013

Lemma. The identity and inverses are unique.

Proof. Suppose that two distinct identities / inverses exist, and show directly that they are equal. □

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

Lemma. The image $\theta(G)$ of a homomorphism $\theta : G \to H$ is a subgroup of H.

Proof. Show that it satisfies the four group axioms, with obvious choices for the identity and inverses. □

Lemma. The composition of two homomorphisms is a homomorphism and similarly for isomorphisms.

Proof. Show that the map respects the group operation. For the isomorphism case, composition of bijections is a bijection. □

Lemma. The inverse of an isomorphism is an isomorphism.

Proof. Show that the inverse map (which exists since it's a bijection) respects the group operation. □

Proposition. $\mathrm{Sym}(X)$ is a group under composition of functions.

Proof. Show that is satisfies the group axioms. (Note: a permutation f of a set X is just a bijection $f : X \to X$.) □

Lemma. If two cycles in S_n are disjoint they commute.

Proof. Consider separately the effect on an element which is permuted by one, the other, or neither cycle. □

Theorem. Every permutation of S_n can be written as a product of disjoint cycles (in an essentially unique way).

Proof. Let $X = \{1, 2, \dots n\}$ and $\sigma \in S_n$. Choose an element a, and consider $a, \sigma(a), \sigma^2(a), \dots$ - then there exists a minimal j such that $\sigma^j(a) = a$ since X is finite. So $(a, \sigma(a), \dots \sigma^{j-1}(a))$ is a cycle in σ. Repeat with $b \in X \setminus \{a, \sigma(a), \dots \sigma^{j-1}(a)\}$ etc. until all elements of X are in a cycle. □

Lemma. $g^n = e$ if and only if $o(g)$ divides n.

Proof. Left to right: use division algorithm to write $n = qm + r$ where $o(g) = m$, then $e = g^{qm+r} = g^r$, implying $r = 0$ by the minimality of m. Right to left is trivial. $\square$

Lemma. For disjoint cycles $\sigma, \tau \in S_n$, $o(\sigma\tau) = \mathrm{lcm}(o(\sigma), o(\tau))$.

Proof. Let $k = \mathrm{lcm}(o(\sigma), o(\tau))$. Then $(\sigma\tau)^k = \sigma^k\tau^k = e$ since σ, τ are disjoint so they commute. Also, if $(\sigma\tau)^n = \sigma^n\tau^n = e$ then $\sigma^n = e$ and $\tau^n = e$ since they permute different elements. So $o(\sigma) \mid n$ and $o(\tau) \mid n$, so $k \mid n$ hence $o(\sigma\tau) = k$. $\square$

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

Proof. Can just consider k-cycles: $(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}\ a_k)$. $\square$

Lemma. The function $\mathrm{sgn}(\sigma) : S_n \to \{\pm 1\}$ is well-defined.

Proof. Show that multiplication by a transposition $\tau = (k\ l)$ changes the parity of $\mathrm{sgn}(\sigma)$, by considering the cases when k and l lie in the same cycle, and in different cycles of σ. $\square$

Theorem. The map $\mathrm{sgn} : (S_n, \circ) \to (\{\pm 1\}, \times) : \sigma \mapsto \mathrm{sgn}(\sigma)$ is a well-defined, non-trivial homomorphism.

Proof. Well-defined: see above. Non-trivial: $\mathrm{sgn}((1\ 2)) = -1$. Homomorphism: let $\alpha = \tau_1 \ldots \tau_a$ and $\beta = \tau'_1 \ldots \tau'_b$ where $\alpha, \beta \in S_n$ and τ_i, τ'_i are transpositions, then

$$\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\tau_1 \ldots \tau_a \tau'_1 \ldots \tau'_b) = (-1)^{a+b} = (-1)^a(-1)^b = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta).$$ $\square$

Corollary. The even permutations of S_n form a subgroup of S_n, denoted A_n, the alternating group.

Proof. Show that it satisfies the four group axioms. $\square$

Proposition. For $n \geq 3$, D_{2n} is a non-abelian group of order $2n$ which naturally embeds into S_n. It is generated by elements σ and τ of orders n and 2 representing a rotation and reflection and hence given by $\{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}, \tau, \sigma\tau \ldots, \sigma^{n-1}\tau\}$.

Proof. The group axioms are clearly true since the elements are symmetries. Labelling the vertices of the n-gon gives a natural embedding into S_n. $\square$

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

Proof. Define $\theta g : H \to gH : h \mapsto gh$, and check that θg is injective and surjective. $\square$

Lemma. The left cosets of H in G form a partition of G.

Proof. Any element g is in gH since $e \in H$. Suppose $c \in aH \cap bH$, and show that $aH = bH = cH$. Now, $c \in aH$, so $\exists k \in H$ such that $c = ak$. So $cH = \{ch : h \in H\} = \{akh : h \in H\} \subseteq aH$ (since $kh \in H$ by closure). Similarly, $a = ck^{-1}$ so $aH \subseteq cH$. Thus $aH = cH$, and similarly $bH = cH$. $\square$

Lemma. Let $H \subseteq G$ and $a, b \in G$. Then $aH = bH$ if and only if $a^{-1}b \in H$.

Proof. Left to right: $b \in aH$ so $b = ak$, some $k \in H$, so $a^{-1}b = k \in H$.

Right to left: $a^{-1}b = k$, some $k \in H$, so $b = ak \in aH$ and $b \in bH$. Since $aH \cap bH \neq \emptyset$, $aH = bH$ (see above). $\square$

Theorem (Lagrange's Theorem)**.** Let H be a subgroup of a finite group G. The order of H divides the order of G.

Proof. G is partitioned into distinct cosets of H, say $G = g_1H \mathbin{\dot\cup} g_2H \mathbin{\dot\cup} \ldots \mathbin{\dot\cup} g_kH$. Since $|g_iH| = |H|$, it is clear that $|G| = k|H|$. □

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

Proof. Consider the subgroup generated by g, which has order $o(g)$, and by Lagrange's Theorem this divides the order of G. □

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

Proof. Let $e \neq g \in G$. Then $o(g) \mid |G| = p$ by Lagrange. Since $o(g) \neq 1$, $o(g) = p$, so $|\langle g \rangle| = p = |G|$, so $\langle g \rangle = G$. □

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

Proof. For $n \in \mathbb{N}$ define $R_n = \{a : 1 \leq a \leq n, \mathrm{hcf}(a, n) = 1\}$ and show that it is a group under $\times_n$: $\mathrm{hcf}(a, n) = \mathrm{hcf}(b, n) = 1 \implies \mathrm{hcf}(ab, n) = 1$ and find inverses by Bezout's Theorem. Then by Lagrange, $\bar{a}^{|R_n|} = 1$, where $\bar{a} = a \bmod n$. But $|R_n| = \phi(n)$, so $a^{\phi(n)} \equiv 1 \bmod n$. □

Proposition. Let $K \leq G$. The following are equivalent definitions of normal subgroup:

i) $gK = Kg \quad \forall g \in G$
ii) $gKg^{-1} = K \quad \forall g \in G$
iii) $gkg^{-1} \in K \quad \forall k \in K, g \in G$

Proof. **(i) ⇒ (ii)** $gKg^{-1} = (gK)g^{-1} = (Kg)g^{-1} = K$
(ii) ⇒ (iii) Trivial.
(iii) ⇒ (i) $gkg^{-1} = k'$, some $k' \in K$, so $gk = k'g$ i.e. $gK \subseteq Kg$. Similarly, $g^{-1}kg = k''$, so $Kg \subseteq gK$. Thus $gK = Kg$.
□

Lemma. If K is a subgroup of G of index 2 then K is normal in G.

Proof. Let $g \in G \setminus K$. Then $G = K \mathbin{\dot\cup} gK$ and $G = K \mathbin{\dot\cup} Kg$ by Lagrange. Hence $gK = Kg \quad \forall g \in G$. □

Theorem. If $K \trianglelefteq G$, the set $(G : K)$ of left cosets of K in G is a group (the quotient group) under coset multiplication.

Proof. Show that coset multiplication is well-defined. Since K is normal in G, $gK = Kg$. Thus, if $gK = \hat{g}K$ and $hK = \hat{h}K$ then $ghK = g\hat{h}K = gK\hat{h} = \hat{g}K\hat{h} = \hat{g}\hat{h}K$.
Then show that the group axioms hold. □

Theorem (First Isomorphism Theorem)**.** Let G, H be groups and $\theta : G \to H$ a group homomorphism. Then $\mathrm{Im}(\theta) \leq H, \mathrm{Ker}(\theta) \trianglelefteq G$ and $G/\mathrm{Ker}(\theta) \cong \mathrm{Im}(\theta)$.

Proof. $\mathrm{Im}(\theta) \leq H$: obvious since θ is a homomorphism.
$\mathrm{Ker}(\theta) \trianglelefteq G$: on example sheet 1; show satisfies group axioms and that $\theta(gkg^{-1}) = e_H$ i.e. $gkg^{-1} \in \mathrm{Ker}(\theta)$.
$G/\mathrm{Ker}(\theta) \cong \mathrm{Im}(\theta)$: construct an isomorphism $\phi : G/\mathrm{Ker}(\theta) \to \mathrm{Im}(\theta) : gK \mapsto \theta(g)$ where $K = \mathrm{Ker}(\theta)$. To show that it is an isomorphism ...

Well-defined: Suppose $gK = hK$, then $h^{-1}g \in K$. Hence by definition, $\theta(h^{-1}g) = e_H$, so $\theta(h)^{-1}\theta(g) = e_H$ since θ is a homomorphism. Thus $\theta(g) = \theta(h)$ and so $\phi(gK) = \phi(hK)$.

Homomorphism: $\phi(gKhK) = \phi(ghK) = \theta(gh) = \theta(g)\theta(h) = \phi(gK)\phi(hK)$.

Surjective: Reverse the argument for well-defined. $\square$

Lemma. A homomorphism $\theta : G \to H$ is injective if and only if $\mathrm{Ker}(\theta) = \{e_G\}$.

Proof. Left to right: Suppose $g \in \mathrm{Ker}(\theta)$, then $\theta(g) = e_H = \theta(e_g)$, so $g = e_G$.
Right to left: Suppose $\theta(g) = \theta(h)$, then $\theta(h^{-1}g) = e_H$. Thus $h^{-1}g \in \mathrm{Ker}(\theta) = \{e_G\}$, so $h = g$. $\square$

Lemma. Let $N \trianglelefteq G$ and $H \leq G$ then $NH \leq G$.

Proof. Show that $NH = \{nh : n \in N, h \in H\}$ satisfies the group axioms. e.g. Closure: For $nh, \bar{n}\bar{h} \in NH$, $nh.\bar{n}\bar{h} = n\hat{n}h\bar{h}$ for some $\hat{n} \in N$ since N normal. $\square$

Lemma. Let $N \trianglelefteq G$, $M \trianglelefteq G$ then $NM \trianglelefteq G$.

Proof. Let $nm \in NM, g \in G$. Then $gnmg^{-1} = gng^{-1}gmg^{-1} \in NM$ since $gng^{-1} \in N$ and $gmg^{-1} \in M$. $\square$

Lemma. Let $(h, k) \in H \times K$. Then $o((h, k)) = \mathrm{lcm}(o(h), o(k))$.

Proof. Let $m = \mathrm{lcm}(o(h), o(k))$. Then $(h, k)^m = (h^m, k^m) = (e, e)$. Suppose $(e, e) = (h, k)^n = (h^n, k^n)$, then $h^n = e$ and $k^n = e$, so $o(h) \mid n$ and $o(k) \mid n$, so $\mathrm{lcm}(o(h), o(k)) \mid n$. $\square$

Corollary. $C_n \times C_m \cong C_{nm}$ if and only if $\mathrm{hcf}(n, m) = 1$.

Proof. By above result, there exists an element in $C_n \times C_m$ of order nm if and only if $\mathrm{hcf}(n, m) = 1$. $\square$

Proposition. 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) $hk = kh \quad \forall h \in H,\ k \in K$

then $G \cong H \times K$ and we call G the *internal* direct product of H and K.

Proof. Define $\theta : G \to H \times K : g = hk \mapsto (h, k)$.

Well-defined: Suppose $g = h_1k_1 = h_2k_2$, then $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$, so $h_1 = h_2$ and $k_1 = k_2$ i.e. the expression $g = hk$ is unique.

Homomorphism: $\theta(g_1g_1) = \theta(h_1k_1h_2k_2) = \theta(h_1h_2k_1k_2) = (h_1h_2, k_1, k_2) = (h_1, k_1)(h_2, k_2) = \theta(g_1)\theta(g_2)$

Surjective: $g = hk \mapsto (h, k)$

Injective: Suppose $\theta(g_1) = \theta(g_2)$, then $(h_1, k_1) = (h_2, k_2)$, so $h_1 = h_2$ and $k_1 = k_2$, thus $g_1 = g_2$. $\square$

Lemma. Suppose G acts on the non-empty set X via ρ. Fix $g \in G$. Then the map $\phi_g : X \to X : x \mapsto \rho(g, x)$ is a permutation.

Proof. ϕ_g is obviously a map, so need to show it is a bijection, or equivalently that it has a 2-sided inverse. For any $x \in X$, we have $\phi_{g^{-1}} \circ \phi_g(x) = \rho(g^{-1}, \rho(g, x)) = \rho(g^{-1}g, x) = \rho(e, x) = x$ and similarly $\phi_g \circ \phi_{g^{-1}}(x) = x$. □

Proposition. Suppose G acts on the set X. Then the map $\Phi : G \to \mathrm{Sym}(X) : g \mapsto \phi_g$ as above is a homomorphism. i.e. $\Phi(gh) = \Phi(g) \circ \Phi(h)$.

Proof. Let $x \in X$. Then $\phi_{gh}(x) = \rho(gh, x) = \rho(g, \rho(h, x)) = \phi_g \circ \phi_h(x)$. □

Theorem (Cayley's Theorem)**.** Any group G is isomorphic to a subgroup of $\mathrm{Sym}(X)$ for some X. e.g. take X to be the elements of G.

Proof. Consider the left regular action $G \times G \to G : (g, h) \mapsto gh$. This is a faithful action (since $gh = h \quad \forall h \in G \implies g = e$). Thus we have an injective homomorphism $\Phi : G \to \mathrm{Sym}(X)$ and $G \lesssim \mathrm{Sym}(G)$. □

Lemma. The distinct orbits form a partition of X.

Proof. Note that for $x \in X$, $x \in \mathrm{Orb}_G(x)$ since $e(x) = x$. Then suppose that $z \in \mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y)$ and show that $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(z) = \mathrm{Orb}_G(y)$. □

Lemma. $\mathrm{Stab}_G(x)$ is a subgroup of G.

Proof. Show that it satisfies the group axioms. □

Theorem (Orbit-Stabiliser Theorem)**.** Let G be a finite group acting on a set X. Let $x \in X$, then $\mathrm{Stab}_G(x) \leq G$ and $|G| = |\mathrm{Stab}_G(x)||\mathrm{Orb}_G(x)|$.

Proof. Prove that $|(G : \mathrm{Stab}_G(x))|$, the number of left cosets of $\mathrm{Stab}_G(x)$ in G is equal to the order of $\mathrm{Orb}_G(x)$.

Let $\theta : (G : \mathrm{Stab}_G(x)) \to \mathrm{Orb}_G(x) : g\mathrm{Stab}_G(x) \mapsto g(x)$.

Check that θ is well-defined: suppose $g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$, then $h^{-1}g \in \mathrm{Stab}_G(x)$, so $h^{-1}g(x) = x$, so $g(x) = h(x)$, i.e. $\theta(g\mathrm{Stab}_G(x)) = \theta(h\mathrm{Stab}_G(x))$.

Show that θ is injective: suppose $\theta(g\mathrm{Stab}_G(x)) = \theta(h\mathrm{Stab}_G(x))$, then $g(x) = h(x)$, so $h^{-1}g(x) = x$, thus $h^{-1}g \in \mathrm{Stab}_G(x)$, so $g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$.

Show that θ is onto: if $g(x) \in \mathrm{Orb}_G(x)$ then $\theta(g\mathrm{Stab}_G(x)) = g(x)$.

Thus θ is a well-defined bijection, so the two sets have equal size. □

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

Proposition. Let p be a prime and G a group of order p^n, some $n \geq 1$. Then $Z(G)$ is non-trivial, i.e. $Z(G) > \{e\}$.

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

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

Theorem. The permutations π and σ in S_n are conjugate in S_n if and only if they are of the same cycle type.

Corollary. 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. $n = n_1+n_2+\ldots+n_k$ with $n_1 \geq n_2 \geq \ldots \geq n_k \geq 1$.

Theorem. A_5 is a simple group (it has no non-trivial proper normal subgroups).

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

Proposition. $\mathrm{Det} : GL_n(\mathbb{R}) \to (\mathbb{R}^*, \times) : A \mapsto \det(A)$ is a surjective homomorphism.

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

Lemma. Let $A \in O_n(\mathbb{R})$ and $x, y \in \mathbb{R}^n$. Then

i) $A\mathbf{x} \cdot A\mathbf{y} = \mathbf{x} \cdot \mathbf{y}$
ii) $|A\mathbf{x}| = |\mathbf{x}|$

Proof. i) $A\mathbf{x} \cdot A\mathbf{y} = (A\mathbf{x})^T(A\mathbf{y}) = \mathbf{x}^T A^T A\mathbf{y} = \mathbf{x}^T\mathbf{y} = \mathbf{x} \cdot \mathbf{y}$
ii) $|A\mathbf{x}|^2 = A\mathbf{x} \cdot A\mathbf{x} = \mathbf{x} \cdot \mathbf{x} = |\mathbf{x}|^2$

□

Proposition. Let $A \in SO_e(\mathbb{R})$. Then A has as eigenvector with eigenvalue 1.

Theorem. Let $A \in SO_3(\mathbb{R})$. Then 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, A is a rotation through an axis through the origin.

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

Proposition. Suppose there exists at least 3 values of $z \in \mathbb{C}$ such that $\dfrac{az+b}{cz+d} = \dfrac{\alpha z+\beta}{\gamma z+\delta}$, with $ad-bc \neq 0$ and $\alpha\delta-\beta\gamma \neq 0$. 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 $\mathbb{C}_\infty$.

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

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

Corollary. $\dfrac{SL_2(\mathbb{C})}{\{\pm I\}} \cong M$

Proposition. Every Möbius map can be written as a composition of maps of the following forms:

i) $f(z) = az, \quad a \neq 0$ — dilatation or rotation
ii) $f(z) = z + b$ — translation

iii) $f(z) = \frac{1}{z}$ inversion

Theorem. The action of M on $\mathbb{C}_\infty$ is sharply triply transitive. i.e. there exists a unique $f \in M$ such that given $x_1, x_2, x_3 \in \mathbb{C}_\infty$ all distinct and $y_1, y_2, y_3 \in \mathbb{C}_\infty$ all distinct, $f(x_i) = y_i$ for $i = 1, 2, 3$.

Theorem. Any non-identity Möbius map is conjugate to one of:

i) $f(z) = \nu z, \quad \nu \neq 0, 1$
ii) $f(z) = z + 1$

Corollary. A non-identity Möbius map f has either 2 fixed points or 1 fixed point.

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

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

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