Groups

Key Theorems and Corollaries

Lectured by Dr Rachel Camina

Michaelmas 2013

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

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

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 $G = g_1H \,\dot{\cup}\, g_2H \,\dot{\cup} \ldots \dot{\cup}\, g_kH$. 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. □

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

Proof. For $n \in \mathbb{N}$ define $R_n = \{a : 1 \leq a \leq n, \text{hcf}(a, n) = 1\}$ and show that it is a group under $\times_n$: $\text{hcf}(a, n) = \text{hcf}(b, n) = 1 \implies \text{hcf}(ab, n) = 1$ 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 $a^{\phi(n)} \equiv 1 \bmod n$. □

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

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

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 $G \lesssim \mathrm{Sym}(G)$. $\square$

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. $\square$

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.

Proof. Let $X = \{(x_1, x_2, \ldots, x_p) : x_i \in G, x_1x_2\ldots x_p = e\}$ (i.e. p-tuples of elements of G such that their product is the identity) - the first $p-1$ elements in the tuple can be freely chosen, then the last is uniquely determined as the inverse of the product of the first $p-1$ elements - thus $|X| = |G|^{p-1}$. Also, let $H = \langle h : h^p = e\rangle \cong C_p$.

Consider the group action $\rho : H \times X \to X : (h^i, x) \mapsto \rho(h^i, x) = (x_{1+i}, x_{2+i}, \ldots, x_{p+i})$ where the suffices are modulo p (i.e. cyclic permutations of the p-tuples). Show that this is a group action:

$x_{1+i}x_{2+i}\ldots x_{p+i} = (x_1\ldots x_i)^{-1}(x_1\ldots x_p)(x_1\ldots x_i) = (x_1\ldots x_i)^{-1}e(x_1\ldots x_i) = e$ so $\rho(h^i, x) \in X$ (or note that $ab = e \implies ba = e$ so cyclic permutations of an element in X give another element in X).

$h^{i+j}(x_1, \ldots, x_p) = (x_{1+i+j}, \ldots, x_{p+i+j}) = h^i(h^j(x_1, \ldots, x_p))$.

$e(x_1, \ldots, x_p) = h^p(x_1, \ldots, x_p) = (x_1, \ldots, x_p)$.

Let $x = (x_1, \ldots, x_p) \in X$. From the Orbit-Stabiliser theorem, $|\mathrm{Orb}_H(x)||\mathrm{Stab}_H(x)| = |H| = p$. Therefore $|\mathrm{Orb}_H(x)| = 1$ or p, since p is prime. The former $(= 1)$ happens only if the x_i are all equal.

Since distinct orbits partition X, the sum of all the distinct orbits is $|X|$. Note that $|\mathrm{Orb}_H((e, e, \ldots, e))| = 1$, so for $|X|$ to be divisible by p, there must be at least $p-1$ other elements with orbits of size 1. Thus there exists $\bar{x} = (x, \ldots, x)$ such that $|\mathrm{Orb}_H(\bar{x})| = 1$ i.e. $x^p = e$. $\square$