2D Groups

State and prove Lagrange's Theorem.

Lagrange's Theorem: If G is a finite group and H a subgroup then $|H|$ divides $|G|$.

Proof: Define a relation $\sim$ on G by $g_1 \sim g_2$ iff $g_1^{-1}g_2 \in H$. This is reflexive (since H contains the identity), symmetric (since $g_2^{-1}g_1 = (g_1^{-1}g_2)^{-1}$ and H is closed under inverses) and transitive (as $g_1^{-1}g_3 = (g_1^{-1}g_2)(g_2^{-1}g_3)$ and H is closed under products). Hence it is an equivalence relation, and G is partitioned into equivalence classes.

We now claim that for each $g \in G$ its equivalence class $[g]$ has size $|H|$, so that

$$|G| = |H| \times \#\textit{equivalence classes}$$

is divisible by $|H|$. Well, define a map $f : [g] \to H$ by $x \mapsto g^{-1}x$.

f well-defined: If $x \in [g]$ then $g^{-1}x \in H$ so $f(x) \in H$.

f bijective: Its inverse is $x \mapsto gx$ (this is similarly well-defined $H \to [g]$).

[6] *Thus $|[g]| = |H|$ and we're done.* $\square$

Show that the dihedral group of order $2n$ has a subgroup of order k for every k dividing $2n$.

The dihedral group D_{2n} is the symmetry group of a regular n-gon in the plane. If $m > 1$ divides n then one can form a regular m-gon with vertices every (n/m)th vertex of the n-gon. The symmetry group of this m-gon (of order $2m$) and its rotational subgroup (of order m) form subgroups of the symmetry group of the n-gon. So we have found subgroups of D_{2n} of order m and $2m$ for every $m > 1$ dividing n, and hence of order k for every $k \mid 2n$ (for $k = 1$ just take the subgroup $\{e\}$,
[4] *and for $k = 2$ the subgroup generated by a reflection).*

---

[10]

5D Groups

(a) Let G be a finite group, and let $g \in G$. Define the *order* of g and show it is finite. Show that if g is conjugate to h, then g and h have the same order.

The order $o(g)$ of g is the smallest positive integer n such that $g^n = e$.

Claim: The order exists (is finite).

Proof: We need to show that the set $\{n > 0 : g^n = e\}$ is non-empty. Let $|G| = N$ and consider the $N+1$ elements of G given by $e, g, g^2, \ldots, g^N$.

By the pigeonhole principle, there exist distinct $i, j \in \{0, 1, \ldots, N+1\}$ with $g^i = g^j$. WLOG $i < j$. Then $g^{j-i} = e$ so $j - i \in \{n > 0 : g^n = e\}$ and we're done. $\square$

Suppose $g = khk^{-1}$. Then for $n \in \mathbb{Z}$ we have $g^n = kh^nk^{-1}$ so

$$g^n = e \iff kh^nk^{-1} = e \iff h^n(= k^{-1}k) = e.$$

[5] *Thus $\{n \in \mathbb{Z} : g^n = e\} = \{n \in \mathbb{Z} : h^n = e\}$ so $o(g) = o(h)$.*

(b) Show that every $g \in S_n$ can be written as a product of disjoint cycles. For $g \in S_n$, describe the order of g in terms of the cycle decomposition of g.

Take any $g \in S_n$; this represents a permutation of $\{1, 2, \ldots, n\}$. For $m \in \{1, 2, \ldots, n\}$ let $i(m)$ be the smallest positive integer with $g^{i(m)}(m) = m$ (this exists since $g^{o(g)}(m) = m$).

Then $m, g(m), \ldots, g^{i(m)-1}(m)$ are distinct: if $g^j(m) = g^k(m)$ with $0 \leqslant j < k < i(m)$ then $g^{k-j}(m) = m$, contradicting minimality of $i(m)$. Moreover they are cycled by the action of g. In particular they are closed under the action of the subgroup of S_n generated by g, so form the orbit of m under this subgroup.

Thus g acts on the orbit of each element m as a cycle. Since distinct orbits are disjoint, we obtain a disjoint cycle decomposition of g.

The order of g is the lcm of the lengths of the cycles in its disjoint
[5] *cycle representation.*

(c) Define the alternating group A_n. What is the condition on the cycle decomposition of $g \in S_n$ that characterises when $g \in A_n$?

Every $g \in S_n$ can be written as a product of transpositions, and the number of transpositions is well-defined mod 2. Say g is <u>even</u> (resp <u>odd</u>) if this number is even (odd). $A_n = \{g \in S_n : g \text{ is even}\}$.

Since a cycle of length k is a product of $k - 1$ transpositions, g lies in A_n iff the number of cycles in its cycle decomp of even length is
[3] *even.*

(d) Show that, for every n, A_{n+2} has a subgroup isomorphic to S_n.

Let τ be the permutation of $\{1, 2, \ldots, n+2\}$ transposing $n+1$ and $n+2$. View perms of $\{1, 2, \ldots, n\}$ as perms of $\{1, 2, \ldots, n+2\}$ in the obvious way. Let $N : S_{n+2} \to \mathbb{Z}/2$ be the homomorphism sending a perm to the mod 2 number of factors in its decomp into transpositions.

Define a map $\theta : S_n \to S_{n+2}$ by

$$\theta(\pi) = \pi\tau^{N(\pi)}.$$

We claim θ is an injective homomorphism with image contained in A_{n+2}, so it defines an isomorphism between S_n and a subgroup of A_{n+2}.

$\underline{\theta \text{ is a hom:}}$ Perms of $\{1,2,\ldots,n\}$ commute with τ, so for $\pi_1, \pi_2 \in S_n$ we have

$$\theta(\pi_1\pi_2) = \pi_1\pi_2\tau^{N(\pi_1\pi_2)} = \pi_1\tau^{N(\pi_1)}\pi_2\tau^{N(\pi_2)} = \theta(\pi_1)\theta(\pi_2).$$

$\underline{\theta \text{ injective:}}$ θ has a left inverse given by restricting perms of $\{1,2,\ldots,n+2\}$ to $\{1,2,\ldots,n\}$.

$\underline{\theta(S_n) \subset A_{n+2}}$: For $\pi \in S_n$ we have

$$N(\theta(\pi)) = N(\pi) + N\big(\tau^{N(\pi)}\big) = 2N(\pi) = 0 \mod 2.$$

[7] *Hence $\theta(S_n)$ is a subgroup of A_{n+2} isomorphic to S_n.*

---

[20]

7D Groups

(a) State the orbit–stabilizer theorem.

(a) <u>Orbit-Stabiliser:</u> If a finite group G acts on a set X then for all $x \in X$ we have

$$|G| = |G \cdot x||G_x|,$$

[1] *where $G \cdot x$ is the orbit of x and G_x the stabiliser.*

Let a group G act on itself by conjugation. Define the centre $Z(G)$ of G, and show that $Z(G)$ consists of the orbits of size 1. Show that $Z(G)$ is a normal subgroup of G.

$Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$. Thus $g \in G$ lies in the centre iff $hgh^{-1} = g$ for all $h \in G$, i.e. iff g is fixed by the conjugation action, so iff the orbit of g has size 1.

$\underline{Z(G) \text{ is a subgroup:}}$ Clearly $e \in Z(G)$. If $g_1, g_2 \in Z(G)$ then for all $h \in G$ we have

$$(g_1g_2)h = g_1hg_2 = h(g_1g_2)$$

using associativity, so $g_1g_2 \in Z(G)$. Finally, for all $g \in Z(G)$ and $h \in G$ we have

$$g^{-1}h = g^{-1}hgg^{-1} = g^{-1}ghg^{-1} = hg^{-1},$$

so $g^{-1} \in Z(G)$.

$\underline{Z(G) \text{ normal:}}$ For $g \in Z(G)$ and $h \in G$ we have $hgh^{-1} = g \in Z(G)$, so $hZ(G)h^{-1} \subset Z(G)$ for all h. Hence $Z(G)$ is normal in G. [5]

(b) Now let $|G| = p^n$, where p is a prime and $n \geqslant 1$. Show that if G acts on a set X, and Y is an orbit of this action, then either $|Y| = 1$ or p divides $|Y|$.

(b) *Let y be an element of Y. Then orbit-stabiliser gives*

$$p^n = |Y||G_y|,$$

[2] *so $|Y|$ divides p^n. Hence $|Y|$ is 1 or divisible by p.*

Show that $|Z(G)| > 1$.

Let G act on itself by conjugation. Then, considering the partition of G into orbits, we get

$$\begin{aligned} |Z(G)| &= \#\textit{orbits of size } 1 \\ &= |G| - \sum_{\substack{\textit{orbits } Y \\ \textit{with } |Y|>1}} |Y| \end{aligned}$$

and each term on the RHS is divisible by p. So $p \mid |Z(G)|$. Since
[5] *$|Z(G)| \geqslant 1$ ($Z(G)$ contains e) we have $|Z(G)| \geqslant p > 1$.*

By considering the set of elements of G that commute with a fixed element x not in $Z(G)$, show that $Z(G)$ cannot have order p^{n-1}.

Suppose $Z(G) \neq G$, and pick $x \in G \setminus Z(G)$. Then $G_x = \{g \in G : gx = xg\}$ is a subgroup of G, and is proper since $x \notin Z(G)$. Moreover $Z(G) \leqslant G_x$ and is proper since $x \in G_x \setminus Z(G)$. We thus have a chain of subgroups

$$Z(G) \lneq G_x \lneq G,$$

and by Lagrange's theorem

$$|Z(G)| \leqslant \frac{|G_x|}{p} \leqslant \frac{|G|}{p^2} = p^{n-2}.$$

[7] *So $|Z(G)|$ cannot be p^{n-1}.*

---

[20]