II.D. Cosets and Lagrange's theorem

II.D.1. DEFINITION. The **order** of a group G is $|G|$, its order as a set. The **order** of an element $a \in G$ is $|\langle a \rangle|$, the order of the cyclic subgroup it generates.

To determine the relation between these orders (in the finite case), we consider more generally $|H|$ for $H \leq G$ and introduce (left) **cosets**

$$aH := \{ah \mid h \in H\} \subset G.$$

These are *not* subgroups.

II.D.2. PROPOSITION. *Distinct cosets are disjoint and have the same number of elements.*

PROOF. First, we claim that

$$aH = bH \iff b^{-1}a \in H \iff a \in bH. \tag{II.D.3}$$

The second "iff" is clear. To see the first, write

$$\begin{aligned} b^{-1}a \in H &\iff \forall h \in H,\ b^{-1}ah =: h' \in H \\ &\iff \forall h \in H,\ ah = bh' \text{ for some } h' \in H \\ &\iff aH \subset bH, \end{aligned}$$

and similarly

$$bh \subset aH \iff a^{-1}b \in H \; (\iff b^{-1}a \in H \text{ since } (a^{-1}b)^{-1} = b^{-1}a).$$

So if $\alpha \in aH$ and $aH \neq bH$, then (by (II.D.3)) $\alpha H = aH \neq bH$, hence (again by (II.D.3)) $\alpha \notin bH$; and we conclude that $aH \cap bH = \emptyset$. Finally, the map (of sets) $H \to aH$ sending $h \mapsto ah$ is a bijection by the cancellation law II.C.1(a). □

Notice that what we have established is that

the left cosets are the partition of G formed by the equivalence relation $a \equiv b \iff b^{-1}a \in H$.

II.D.4. LAGRANGE'S THEOREM. *For $H < G$ with $|G| < \infty$, we have $|H| \big| |G|$. In particular, the order of any $a \in G$ divides G.*

II.D.5. DEFINITION. $[G{:}H] := \frac{|G|}{|H|} \in \mathbb{N}$ is called the **index** of H in G, and is the number of cosets (as will be clear from the next proof).

PROOF OF II.D.4. We can write

$$G = a_1 H \amalg \cdots \amalg a_r H$$

as a disjoint union. (Why? Every g is in some coset, namely gH. Write $G = \cup_{g \in G} gH$ and strike out repeated cosets. Once there is no repetition, the remaining cosets are disjoint by Prop. II.D.2.) Moreover, we have that $|a_i H| = |1H| = |H|$ for all i (also by Prop. II.D.2). So $|G| = \sum_{i=1}^{r} |a_i H| = r|H|$. $\square$

II.D.6. EXAMPLES. (a) $G = \mathfrak{S}_3 > H = \langle (12) \rangle = \{1, (12)\}$, $(13)H = \{(13), (13)(12)\} = \{(13), (123)\}$, and $(23)H = \{(23), (132)\}$. Of course, $[G{:}H] = 3$.
(b) If we take $G = D_n > K = \langle r \rangle = \{1, r, r^2, \ldots, r^{n-1}\}$, the only other coset is $hK = \{h, hr, hr^2, \ldots, hr^{n-1}\}$; and $[G{:}H] = 2$.
(c) Suppose p is prime. Since $|D_p| = 2p$, the possible orders of elements are 1, 2, p, and $2p$ (though in fact, no element of order $2p$ exists).

Turning to consequences of Lagrange's Theorem, first it should be underscored why we call $|\langle a \rangle|$ the "order of a": consider the sequence of powers $1, a, a^2, \ldots, a^k$, with k the least power for which one has a repetition (i.e. $a^k \in \{1, a, a^2, \ldots, a^{k-1}\}$). Then multiplying $a^k = a^i$ by a^{-i} gives $a^{k-i} = 1$, contradicting the leastness of k unless $i = 0$. Hence $a^k = 1$, and $1, a, a^2, \ldots, a^{k-1}$ are *distinct*. Moreover, by the Division Algorithm we may write (with $0 \leq r \leq k$)

$$a^m = a^{kq+r} = (\overset{1}{\cancel{a^k}})^q a^r = a^r \in \{1, a, \ldots, a^{k-1}\}$$

for any $m \in \mathbb{Z}$; and so $\langle a \rangle = \{1, a, a^2, \ldots, a^{k-1}\} \implies |\langle a \rangle| = k$.

Now we can deduce

II.D.7. COROLLARY. *Given $a \in G$, with $|G| < \infty$, we have:* (i) *the smallest $k \in \mathbb{Z}_{>0}$ for which $a^k = 1$ divides $|G|$; and* (ii) $a^{|G|} = 1$.

PROOF. (i) is immediate from Lagrange and the discussion above; and (ii) follows since $a^{|G|} = a^{[G:\langle a\rangle]\cdot|\langle a\rangle|} = \big(\cancelto{1}{a^{|\langle a\rangle|}}\big)^{[G:\langle a\rangle]} = 1.$ $\square$

II.D.8. COROLLARY. *If $|G| = p$ is prime, the G is cyclic (hence also abelian).*

PROOF. Let $a \in G \setminus \{1\}$. Since $|\langle a\rangle| > 1$ and $|\langle a\rangle| \big| |G|{=}p$, we must have $|\langle a\rangle| = p$. So a generates G. $\square$

Euler's *phi-function* $\phi(m)$ counts the number of integers between 0 and m which are relatively prime to m; that is, $\phi(m) = |\mathbb{Z}_m^*|$. So applying Corollary II.D.7(ii) to $G = \mathbb{Z}_m^*$ gives

II.D.9. EULER'S THEOREM. *Let $m \geq 2$. In $\mathbb{Z}_m^*$, we have $\bar{a}^{\phi(m)} = \bar{1}$. (That is, $a^{\phi(m)} \underset{(m)}{\equiv} 1$ for any a with $(a, m) = 1$.)*

A special case of this is *Fermat's little theorem*:

$$a^{p-1} \underset{(p)}{\equiv} 1 \quad \text{for } p \text{ prime.} \tag{II.D.10}$$

II.D.11. EXAMPLE. Some subgroups of $\mathfrak{S}_4$ and their orders:

- $V = \{1, (12)(34), (13)(24), (14)(23)\}$ "Klein 4-group"; $|V| = 4$.
- $D_4 < \mathfrak{S}_4$: think of actions of symmetries of a square on the vertices (numbered $1, 2, 3, 4$); $|D_4| = 8$.
- $\mathfrak{A}_4$ alternating group; $|\mathfrak{A}_4| = 12$.

To see the order of $\mathfrak{A}_4$, recall that $|\mathfrak{S}_4| = 4! = 24$; it suffices to show that $[\mathfrak{S}_4{:}\mathfrak{A}_4] = 2$. This is true for *any* n, not just 4: multiplying by any transposition gives a bijection between $\mathfrak{A}_n$ and $\mathfrak{S}_n \backslash \mathfrak{A}_n$.

Since the elements of V have sgn 1 (why?), we have $\mathfrak{S}_n > \mathfrak{A}_n > V$. These elements also arise from symmetries of the square (which ones?), and so $\mathfrak{S}_n > D_n > V$. All of this agrees with Lagrange, which also tells us that neither of $\mathfrak{A}_4$ and D_4 can contain the other.

II.D.12. DEFINITION. The **exponent** of a finite group G is

$$\exp(G) := \min\{e \in \mathbb{N} \mid g^e = 1 \ (\forall g \in G)\}.$$

For example, $\exp(\mathfrak{S}_n) = \text{lcm}[1, \ldots, n]$. When $n = 4$ this is 12: the elements of $\mathfrak{S}_4$ have orders 1, 2, 3, and 4; so the smallest power that makes *all* of them 1 is 12. There is *no* element of actual order 12. (You will check all of this in HW.) The next result says that we can blame this on the fact that $\mathfrak{S}_4$ is nonabelian:

II.D.13. PROPOSITION. *Let G be finite abelian. Then there exists a $g \in G$ with order* $\exp(G)$.

II.D.14. LEMMA. *Let G be abelian. Then for all $g_1, g_2 \in G$,*

$$(|\langle g_1 \rangle|, |\langle g_2 \rangle|) = 1 \implies |\langle g_1 g_2 \rangle| = |\langle g_1 \rangle||\langle g_2 \rangle|.$$

PROOF. As the intersection $\langle g_1 \rangle \cap \langle g_2 \rangle$ is a subgroup of both $\langle g_1 \rangle$ and $\langle g_2 \rangle$, its order divides them both, hence must be 1. Write $o := |\langle g_1 g_2 \rangle|$. Since G is abelian, $(g_1 g_2)^o = 1 \implies g_1^o g_2^o = 1 \implies g_1^o = g_2^{-o} \in \langle g_1 \rangle \cap \langle g_2 \rangle = \{1\}$. Now $g_1^o = 1 = g_2^o$ means that $|\langle g_1 \rangle|$ and $|\langle g_2 \rangle|$ divide o (why?), and so their lcm — which in this case[6] is just $|\langle g_1 \rangle||\langle g_2 \rangle|$ — must also divide o. Again using that G is abelian, we have $(g_1 g_2)^{|\langle g_1 \rangle||\langle g_2 \rangle|} = 1$, and it follows that o divides $|\langle g_1 \rangle||\langle g_2 \rangle|$. So they are equal. $\square$

PROOF OF II.D.13. Let g be an element of maximal order. Suppose $|\langle g \rangle| \neq \exp(G)$, i.e. that there exists $h \in G$ with $h^{|\langle g \rangle|} \neq 1$. Then $|\langle h \rangle|$ does not divide $|\langle g \rangle|$, and there exists a prime p with highest powers p^f resp. p^e dividing $|\langle h \rangle|$ resp. $|\langle g \rangle|$, such that $f > e$. Hence by II.D.14

$$\gamma := \underbrace{h^{|\langle h \rangle| / p^f}}_{\text{order } p^f} \cdot \underbrace{g^{p^e}}_{\text{order } \frac{|\langle g \rangle|}{p^e}} \quad \text{has order } p^{f-e}|\langle g \rangle| > |\langle g \rangle|,$$

in contradiction to the assumed maximality of $|\langle g \rangle|$. $\square$

II.D.15. COROLLARY. *Let G be a finite group. Then*

$$G \textit{ is cyclic} \iff \exp(G) = |G| \textit{ and } G \textit{ is abelian}.$$

PROOF. ($\implies$) is clear: consider a generator of G. For ($\impliedby$), II.D.13 provides $g \in G$ with $|\langle g \rangle| = \exp(G)$ $(= |G|)$. Conclude that $\langle g \rangle = G$. $\square$

[6]Recall that $\mathrm{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$.