Section 10: Counting the Elements of a Finite Group

Let G be a group and H a subgroup. Because the right cosets are the family of equivalence classes with respect to an equivalence relation on G, it follows that the right cosets of H in G form a partition of G (and similarly for the left cosets). Each right coset has the same cardinality as H itself, because $H \to Ha : h \mapsto ha$ is one-to-one and onto. Moreover (and this is almost the only time that we will use both the left and right cosets at the same time), there is a one-to-one correspondence from the set of right cosets to the set of left cosets, given by $Ha \mapsto a^{-1}H$. (It is necessary to throw in the inverse here to make the correspondence well-defined: If $Ha = Hb$, then we may have $aH \neq bH$, but because $ab^{-1} \in H$, we also have $(b^{-1})^{-1}a^{-1} = ba^{-1} = (ab^{-1})^{-1} \in H$, and hence $a^{-1}H = b^{-1}H$. For an example of this, see the last example in the notes for Section 9: We have $\langle g\rangle f = \langle g\rangle f^4 g$, $f\langle g\rangle \neq f^4 g\langle g\rangle$ and $f^{-1}\langle g\rangle = f^4\langle g\rangle = f^4 g\langle g\rangle = (f^4 g)^{-1}\langle g\rangle$.) Thus the cardinalities of the sets of right cosets and left cosets are equal. We denote this common cardinality by $[G : H]$ and call it the *index of H in G*. If G is a finite group, then this index is surely finite; if G is infinite, then it could be finite or infinite. ($[\mathbb{Z} : 5\mathbb{Z}] = 5$; $[\mathbb{Q} : \mathbb{Z}]$ is infinite.)

Suppose now that G is a finite group, with a subgroup H. Then $[G : H]$ is also finite, say n, and, picking one element a_i, $i = 1, 2, \ldots, n$, from each of the right cosets of H in G, we get

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_n| = n|H| \ .$$

(A set like $\{a_1, a_2, \ldots, a_n\}$, one from each coset, is called a "set of coset representatives" of H; such a set doesn't have much structure — it's usually just a convenient way to list the cosets of H.) We've proved a useful and important theorem:

Lagrange's Thm: Let H be a subgroup of a finite group G. Then $|G| = |H|[G : H]$. In particular, the order of any subgroup or element of G divides the order of G.

Ex: For any cyclic group $\langle x\rangle$ with order n and any divisor d of n, there is exactly one subgroup $\langle x^{n/d}\rangle$ of order d.

Ex: Q_8 has one subgroup of order 1 ($\langle I\rangle$), one of order 2 ($\langle -I\rangle$), three of order 4 ($\langle J\rangle$, $\langle K\rangle$, and $\langle L\rangle$), and one of order 8 (Q_8 itself).

Ex: $\mathcal{S}_n$ has order $n!$, and it has elements of orders 1 through n, namely 1-cycles, 2-cycles, and so on up to n-cycles. It also has subgroups of $2n$, namely D_n, and $n!/2$, namely $\mathcal{A}_n$.

A fair question is: If d is a factor of $|G|$, must there be at least one subgroup of order d? It turns out there is such a subgroup <u>if</u> d is a power of a prime number; but for a general d there may not be a subgroup. In particular, we'll see that A_4, which has $4!/2 = 12$ elements, has no subgroup of 6 elements.

Cor: If a group has order a prime number, then the group is cyclic, generated by any non-identity element of the group.

Pf: Let G be a group for which $|G| = p$, a prime number, and let $g \in G - \{e\}$. Then $\langle g\rangle$ is a nontrivial subgroup of G, and its order divides $|G| = p$, so its order <u>is</u> p, so $\langle g\rangle = G$.//

Here is a general result, also a corollary of Lagrange's theorem, that yields as a corollary a result named for Euler, which in turn yields as a corollary a result named for Fermat. The proofs, as befits corollaries, are very short: First, the order of every element in a finite group divides the order of the group. Second, the set of elements of $\mathbb{Z}_n$ that are relatively prime to n form a group under multiplication mod n; the number of such elements, i.e., the order of this group, is denoted by $\varphi(n)$ and called the "Euler phi-function" of n. Third, if n is a prime p, then the only element of $\mathbb{Z}_p$ that is not relatively prime to p is 0, so $\varphi(p) = p - 1$. And recall that "$a \equiv b \mod n$" means that the integers a, b have the same remainder on long division by the positive integer n; i.e., that a, b represent the same element of $\mathbb{Z}_n$.

Cor: If G is a finite group, then for every x in G, $x^{|G|} = e$.

Euler's Thm: If k is an integer relatively prime to the positive integer n, then $k^{\varphi(n)} \equiv 1 \mod n$.

Fermat's Thm: If k is an integer not divisible by the prime p, then $k^{p-1} \equiv 1 \mod p$.

So, for example, for every element f of $\mathcal{S}_n$, $f^{n!} = e$; and because $\varphi(6) = 2$, $19^2 \equiv 1 \mod 6$; and $25^6 \equiv 1 \mod 7$.

Another handy equation for establishing facts about a finite group is called the class equation of the group. Again, it will follow quickly once we have set up the "machinery" that goes into it. We begin with a fact that may have already suggested itself to you. Recall that we say an element g of a group G is called conjugate (in G) to another element h if there is an element x of G for which $xgx^{-1} = h$. The proof of the following result is a good exercise.

Lemma: "Is conjugate (in G) to" is an equivalence relation on G.

Hence, G is partitioned into "conjugacy classes", each consisting of the elements that are conjugate to each other. Unlike cosets, these conjugacy classes need not have the same number of elements; but at least there is a way to write down how many elements there are in a given conjugacy class. Recall that, if g is an element of a group G, then the set of elements x of G that commute with g, i.e., for which $xg = gx$, forms a subgroup $Z(g)$ called the centralizer of g.

Lemma: Two elements x, y of G have the property that $xgx^{-1} = ygy^{-1}$ iff x, y are in the same left coset of $Z(G)$ in G. Hence, the number of elements in the conjugacy class of g is equal to the index $[G : Z(g)]$ (and hence, if G is finite, it divides $|G|$).

Pf: The first sentence just uses the definition of left coset:

$$xgx^{-1} = ygy^{-1} \quad \Leftrightarrow \quad y^{-1}xg = gy^{-1}x \quad \Leftrightarrow \quad y^{-1}x \in Z(g) \quad \Leftrightarrow \quad xZ(g) = yZ(g) \ .$$

The second sentence follows immediately, because all the elements of a given left coset of $Z(g)$ conjugate g to the same element of G, and different cosets correspond to different conjugates of g.//

Now to say that an element g of G has only one conjugate (which must be itself) is to say that G commutes with every element of G, i.e., that $g \in Z(G)$, the center of G. Thus, $Z(G)$ is the union of all the one-element conjugacy classes in G.

Class Equation: Let G be a finite group, and take one element $g_1, g_2, \ldots, g_s$ out of each of the conjugacy classes of G that have at least two elements. Then

$$|G| = |Z(G)| + \sum_{i=1}^{s} [G : Z(g_i)] \ .$$

Pf: Because the conjugacy classes partition G, we know that the order of G is the sum of the cardinalities of all of the conjugacy classes. If we group together the one-element conjugacy classes into $Z(G)$, each of the remaining conjugacy classes has at least two elements, and we have chosen one of these elements to be g_i, say. And we have seen above that the cardinality of the conjugacy class containing g_i is the index of $Z(g_i)$ in G.//

It is useful to note that we have specifically arranged in this equation that none of the indices $[G : Z(g_i)]$ is a 1. Let us look at one example, and then prove a result using this equation.

Ex: In D_6, the only elements that commute with every element are e, f^3, so they constitute $Z(D_6)$. Now $gfg^{-1} = gfg = f^5gg = f^5$, so f, f^5 are in the same conjugacy class. Now $Z(f)$ contains f itself and hence all of $\langle f\rangle$ (including $\langle f^3\rangle = Z(D_6)$), but it is not all of D_6, so $|Z(f)|$ is divisible by $|\langle f\rangle| = 6$ and properly divides $|D_6| = 12$, i.e., it is 6; and so the cardinality of the conjugacy class containing f is $[D_6 : Z(f)] = 12/6 = 2$; i.e., this class is $\{f, f^5\}$. Similarly, $\{f^2, f^4\}$ is another conjugacy class. And $Z(g)$ contains $Z(D_6)$ and g and is not all of D_6, so its order, a proper divisor of 12 divisible by $|\{e, f^3, g, f^3g\}| = 4$, is 4; and hence the number of conjugates of g is $[D_6 : Z(g)] = 12/4 = 3$. We have $fgf^{-1} = f^2g$ and $f^2gf^{-2} = f^4g$, so that the conjugacy class of g is $\{g, f^2g, f^4g\}$. And the remaining conjugacy class is $\{fg, f^3g, f^5g\}$. We have sorted all the elements into their conjugacy classes, and one set of representatives of the conjugacy classes that have more than one element is $\{f, f^2, g, fg\}$:

$$\begin{aligned} D_6 &= \{e, f^3\} \cup \{f, f^5\} \cup \{f^2, f^4\} \cup \{g, f^2g, f^4g\} \cup \{fg, f^3g, f^5g\} \\ |D_6| &= |Z(D_6)| + [D_4 : Z(f)] + [D_5 : Z(f^2)] + [D_5 : Z(g)] + [D_6 : Z(fg)] \\ 12 &= 2 + 2 + 2 + 3 + 3\ . \end{aligned}$$

That last equation was not very interesting, so it may be hard to see what good the class equation does. Here's one use of it in proving a useful fact:

Prop: If $|G|$ is a power of a prime number, then $Z(G)$ is not trivial. If $|G|$ is the square of a prime number, then G is abelian.

Pf: Suppose first that $|G| = p^n$ where p is a prime. Then both $|G|$ and all of the $[G : Z(g_i]$ in the class equation are powers of p, the only divisors of p^n, and none of the factors $[G : Z(g_i)]$ are 1, so they are all divisible by p. Thus, the only remaining term in the class equation, $|Z(G)|$, must be divisible by p also, so $Z(G)$ cannot be trivial.

Now suppose that $|G| = p^2$. We have just shown that $Z(G)$ has either p or p^2 elements, and we want to prove it must be p^2. So assume not, by way of contradiction, and take an element g in $G - Z(G)$. Then $Z(g)$ contains at least $Z(G)$ and g; so it has more than p elements, and hence it has p^2 elements. But that means g commutes with every element of G, i.e., $g \in Z(G)$, contradicting our choice of g and completing the proof.//

Thus, with a little more work, we can show that the only essentially different groups of order (cardinality) a square of a prime p are $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.

Lemma: If $(k_1, k_2, \ldots, k_r)$ is an r-cycle in $\mathcal{S}_n$ and $\varphi \in \mathcal{S}_n$, then

$$\varphi \circ (k_1, k_2, \ldots, k_r) \circ \varphi^{-1} = (\varphi(k_1), \varphi(k_2), \ldots, \varphi(k_r))\ , \qquad (*)$$

another r-cycle. Thus, if two elements of $\mathcal{S}_n$ are conjugate in a subgroup of $\mathcal{S}_n$, then their disjoint cycle decompositions have the same numbers of r-cycles for each positive integer r. The converse is true in $\mathcal{S}_n$ (but it may not be true in a subgroup, because the φ that is necessary to conjugate one element into another with a "matching" disjoint cycle decomposition may not exist in the subgroup).

Pf: We show that both sides of $(*)$ have the same effect on an element j of $\{1, 2, \ldots, n\}$, considering two cases: where j is one of the $\varphi(k_i)$'s, $i = 1, \ldots, r$, and where j is not one of the $\varphi(k_i)$'s. If $j = \varphi(k_i)$, then clearly the right side of $(*)$ takes it to $\varphi(k_{i+1})$; while the left side takes it, first to k_i, then to k_{i+1} [or to k_1, if $i = r$ — we won't bother to mention this case again], then to $\varphi(k_{i+1})$; so the results are the same in this case. If j is not one of the $\varphi(k_i)$'s, then the right side of the equation takes it to itself; while the left side takes it first to $\varphi^{-1}(j)$ — which is not one of the k_i's, because φ^{-1} is one-to-one — then to $\varphi^{-1}(j)$ again (because it is not one of the k_i's, so the r-cycle doesn't move it), then to $\varphi(\varphi^{-1}(j)) = j$; so the results are also the same in this case. Equation $(*)$ follows.

Thus, if an element α of $\mathcal{S}_n$ can be written as $\alpha = \gamma_1\gamma_2 \ldots \gamma_s$ where the γ_i's are disjoint cycles, then

$$\varphi\alpha\varphi^{-1} = (\varphi\gamma_1\varphi^{-1})(\varphi\gamma_2\varphi^{-1}) \ldots (\varphi\gamma_s\varphi^{-1}) ,$$

and by equation $(*)$ each of the $(\varphi\gamma_i\varphi^{-1})$'s is a cycle of the same length as the corresponding γ_i; and the $(\varphi\gamma_1\varphi^{-1})$'s are still disjoint because φ is one-to-one.

For the converse in the context of $\mathcal{S}_n$, suppose we have two elements α, β for which the disjoint cycle decompositions have the same number of cycles of each length. Then if we arrange the cycles in both factorizations so that, say, the 1-cycles come first, the 2-cycles next, the 3-cycles next, and so on, and then let φ be the function that assigns the first entry that appears in α to the first in β, the second in α to the second in β, and so on, then we will have $\varphi\alpha\varphi^{-1} = \beta$.//

To see by example how the construction of the necessary φ in the last paragraph would work, let us take $\alpha = (1, 2)(3, 4, 5) = (6)(7)(1, 2)(3, 4, 5)$ and $\beta = (4)(6)(3, 1)(2, 5, 7)$ in $\mathcal{S}_7$. If we set

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 7 & 4 & 6 \end{pmatrix} ,$$

then we have $\varphi\alpha\varphi^{-1} = \beta$. But we can write α and β in many different ways, even without disturbing the setup where the 1-cycles come first, the 2-cycles next, etc. If we rewrite β as $(6)(4)(1, 3)(5, 7, 2)$, then the method above gives a new φ, namely

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 7 & 2 & 6 & 4 \end{pmatrix} ,$$

and we still have $\varphi\alpha\varphi^{-1} = \beta$. (Apparently the old φ and the new one are in the same left coset of the centralizer of α.) So the φ is not unique, and we <u>may</u> be able to pick one that has some other property, e.g., one that is in some subgroup G of $\mathcal{S}_n$ that also contains α, β, so that α, β are also conjugate in G.

Ex: It is left to the students of combinatorics in the class to see that, in $\mathcal{S}_5$, the cardinalities of the conjugacy classes are as follows:

- the cardinality of the single-element class $\{e\}$ is 1;
- the 2-cycles form a conjugacy class of $(5 \cdot 4)/2 = 10$ elements;
- the 3-cycles form a conjugacy class of $(5 \cdot 4 \cdot 3)/3 = 20$ elements;

- the 4-cycles form a conjugacy class of $(5 \cdot 4 \cdot 3 \cdot 2)/4 = 30$ elements;
- the 5-cycles form a conjugacy class of $5!/5 = 24$ elements;
- the products of two disjoint 2-cycles form a conjugacy class of $(5 \cdot 4 \cdot 3 \cdot 2)/(2 \cdot 2 \cdot 2) = 15$ elements;
- the products of a 3-cycle and a 2-cycle which are disjoint form a conjugacy class of $5!/(3 \cdot 2) = 20$ elements;

so the class equation for $\mathcal{S}_5$ is

$$120 = 1 + 10 + 20 + 30 + 24 + 15 + 20 \ .$$