It will be convenient to make use of the following notation: if d and m are integers then

"$d \mid m$" means "d is a divisor of m".

That is, $d \mid m$ if and only if there exists an integer k such that $m = kd$. Note that $d \mid 0$ is true for all d, since $0 = 0d$. On the other hand, $0 \mid m$ is only true if $m = 0$.

We also use "$d \nmid m$" to mean "d is not a divisor of m."

The introduction of this notation provides a good excuse for restating the two main theorems of group theory that we have done so far.

Lagrange's Theorem: *If H is a subgroup of the finite group G then $\#H \mid \#G$.*

Sylow's Theorem: *Let G be a finite group and p a prime number, and let $\#G = p^k m$, where $p \nmid m$. Let d be the number of subgroups of G of order p^k. Then $d \mid m$, and $d \equiv 1 \pmod{p}$.*

An important corollary of Lagrange's Theorem is that if g is an element of the finite group G then $\text{Order}(g) \mid \#G$. (Recall that the word "order" has two different meanings in group theory. On the one hand, if G is a group then $\#G$, the number of elements of G, is called the order of G. On the other hand, if g is an element of a group then the order of g is the least positive integer n such that g^n is the identity element. The two usages are related by the fact that each element $g \in G$ generates a cyclic subgroup, $\langle g \rangle$, and whose order is equal to the order of g. The corollary mentioned above follows immediately from this , since Lagrange's Theorem tells us that $\#\langle g \rangle \mid \#G$.)

In this week's computer tutorial you were asked to list all the elements of a certain group G of order 12, and then find a subgroup of G of order 4. Note that Sylow's Theorem guarantees that such a subgroup exists. If H is a subgroup of G with $\#H = 4$ then, as we have just noted, the order of any element of H will have to be a divisor of 4. In the tutorial question it happens that eight of the twelve elements of G have order 3, and so cannot possibly lie in any subgroup of order 4. So the H consists of the remaining four elements: the identity (of order 1) and three elements of order 2.

Let us illustrate the proof of Sylow's Theorem in one more case. Specifically, let us show that a group of order 24 must have at one subgroup of order 8.

Let G be a group with $\#G = 24$. Our task is to show that at least one of the $\binom{24}{8}$ subsets of G with eight elements is a subgroup of G. In fact, an odd number of these subsets are subgroups.

The first thing to observe is that the number $\binom{24}{8}$ is odd. Indeed,

$$\binom{24}{8} = \frac{24!}{8!16!} = \frac{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17}{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}$$

and the powers of 2 occurring as factors of numbers in the numerator of this expression are matched exactly by those occurring as factors of numbers in the denominator. For each i from 0 to 7, the highest power of 2 that is a factor of $24 - i$ is the same as the highest power of 2 that is a factor of $8 - i$. Cancelling all these 2's leaves

$$\binom{24}{8} = \frac{3 \cdot 23 \cdot 11 \cdot 21 \cdot 5 \cdot 19 \cdot 9 \cdot 17}{1 \cdot 7 \cdot 3 \cdot 5 \cdot 1 \cdot 3 \cdot 1 \cdot 1}$$

and given that this is an integer it is undoubtedly odd, since it is a ratio of odd numbers. (The actual value is 735471.)

Let $\mathscr{S}$ be the set of all 8-element subsets of G. We have just shown that $\#\mathscr{S}$ is odd. We define a relation $\sim$ on $\mathscr{S}$ by the rule that if $X, Y \in \mathscr{S}$ then $X \sim Y$ if and only if X is a right translate of Y. We know from earlier work that $\sim$ is an equivalence relation. Furthermore, for each $X \in \mathscr{S}$ the number of elements in the equivalence class containing X is the number of right translates of X, and this equals $\#G/\#\mathrm{Stab}(X) = 24/\#\mathrm{Stab}(X)$, where $\mathrm{Stab}(X) = \{\, g \in G \mid Xg = X \,\}$. In particular, the number of elements in any equivalence class must be a divisor of 24.

If X is any nonempty subset of G then the right translates of X must cover G, in the sense that if g is any element of G then there is some $h \in G$ such that $g \in Xh$. Indeed, since X is nonempty we may choose an element $x \in X$, and now defining $h = x^{-1}g$ gives $g = xh \in Xh$. Now if X has eight elements then all the translates of X also have eight elements, and you need at least three sets with eight elements to cover a set with twenty-four elements. So the number of translates of X is a divisor of 24 that is at least 3. That is, it must be 24, 12, 8, 6, 4 or 3.

The 735471 elements of $\mathscr{S}$ are divided into equivalence classes, and since equivalence classes are necessarily pairwise disjoint it follows that 735471 is the sum of the numbers of elements in the various equivalence classes. Since you cannot write an odd number as a sum of even numbers, at least one of the equivalence classes must have an odd number of elements. But 3 is the only odd number in our list of possibilities for the number of elements in an equivalence class; so there is at least one equivalence class having exactly three elements.

We have now shown that there exists an eight-element subset X of G having exactly three right translates. Since these three sets cover G they must be pairwise disjoint. As we proved last week, it follows that one of these translates must be a subgroup.

Homomorphisms

Let G and H be sets, and let $*$ be a binary relation on G and $\circ$ a binary relation on H. A function $\phi\colon G \to H$ is called a *homomorphism* from $(G, *)$ to $(H, \circ)$ if $\phi(x * y) = \phi(x) \circ \phi(y)$ for all $x, y \in G$.

Example 1. Let $G = \mathbb{R}$ (the set of all real numbers) and $*$ the operation of addition, and let $H = \mathbb{R}$ also, and $\circ$ the operation of multiplication. Define $\phi\colon \mathbb{R} \to \mathbb{R}$ by $\phi(x) = 2^x$. Then for all $x, y \in R$,

$$\phi(x + y) = 2^{x+y} = 2^x 2^y = \phi(x)\phi(y),$$

and so ϕ is a homomorphism from $\mathbb{R}$ with addition as the operation to $\mathbb{R}$ with multiplication as the operation.

Example 2. Let ψ be the function from $\mathrm{Mat}_n(\mathbb{R})$ (the set of all $n \times n$ matrices over $\mathbb{R}$) to $\mathbb{R}$ given by $\psi(X) = \det(X)$ (the determinant of X) for all $X \in \mathrm{Mat}_n(\mathbb{R})$. We know from junior level linear algebra that $\det(XY) = \det(X)\det(Y)$ holds for all $n \times n$ matrices X and Y. That is, $\psi(XY) = \psi(X)\psi(Y)$ for all $X, Y \in \mathrm{Mat}_n(\mathbb{R})$. So ψ is a homomorphism from $\mathrm{Mat}_n(\mathbb{R})$ under matrix multiplication to $\mathbb{R}$ under multiplication.

Example 3. Let $S = \mathrm{Sym}(n)$ and let $\varepsilon\colon S \to \{1, -1\}$ be defined by

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Permutation multiplication is an operation on S, and ordinary multiplication of numbers defines an operation on $\{1, -1\}$ (since it is trivial that $\{1, -1\}$ is closed under multiplication). Note that in fact S and $\{1, -1\}$ are groups under these operations. Since $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ for all σ, $\tau \in S$ we see that ε is a homomorphism from the group S to the group $\{1, -1\}$.

Of course, we are primarily interested in homomorphisms between groups.

Homomorphisms in group theory are the analogue of linear transformations in vector space theory. More generally, it is very common in mathematics to investigate sets that are equipped with with some kind of extra structure, and then it is natural to consider functions that preserve this extra structure. Homomorphisms are the structure-preserving functions of group theory, and as such they are of fundamental importance in the subject.

If G and H are any groups then there is always a homomorphism $\phi\colon G \to H$ given by $\phi(x) = e_H$, the identity element of H, for all $x \in G$. These are trivial homomorphisms. Non-trivial homomorphisms should be regarded as rather special, since they always carry significant information concerning the group-theoretic structure of the groups in question. For example, we shall prove that if $\phi\colon G \to H$ is a homomorphism then the set of all $x \in G$ such that $\phi(x) = e_H$ is necessarily a subgroup G.

Lemma. *Let G be a group and $x \in G$. If $x^2 = x$ then x is the identity element of G.*

Proof. Let e be the identity element. If $x^2 = x$ then

$$e = x^{-1}x = x^{-1}x^2 = (x^{-1}x)x = ex = x,$$

as claimed. □

Theorem. *Let G and H be groups and $\phi\colon G \to H$ a homomorphism. Then*

(i) $\phi(e_G) = e_H$, where e_G and e_H are the identity elements of G and H;
(ii) $\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$;
(iii) the set $K = \{\, x \in G \mid \phi(x) = e_H \,\}$ is a subgroup of G;
(iv) the set $I = \{\, \phi(g) \mid g \in G \,\}$ is a subgroup of H.

Proof. Let $h = \phi(e_G) \in H$. Then

$$h^2 = \phi(e_G)\phi(e_G) = \phi(e_G e_G) = \phi(e_G) = h,$$

and it follows from the lemma that $h = e_H$. So $\phi(e_G) = e_H$, proving Part (i).

Let $x \in G$ be arbitrary. Then

$$\phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(e_G) = e_H,$$

and so it follows that $\phi(x^{-1})$ is the inverse of $\phi(x)$. This proves Part (ii).

To prove Part (iii) we must show that K satisfies SG1, SG2 and SG3. For SG1, let x, $y \in K$ be arbitrary. Then $\phi(x) = e_H$ and $\phi(y) = e_H$; so

$$\phi(xy) = \phi(x)\phi(y) = e_h e_h = e_H,$$

and thus $xy \in K$. Since x and y were arbitrary elements of K this shows that K is closed under multiplication. That is, (SG1) holds.

It is immediate from Part (i) that K satisfies (SG2): since $\phi(e_G) = e_H$, the definition of K yields that $e_G \in K$.

It is almost immediate from Part (ii) that K satisfies SG3. For if $x \in K$ is arbitrary, then $\phi(x) = e_H$, and so

$$\phi(x^{-1}) = \phi(x^{-1})e_H = \phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(e_G) = e_H.$$

Thus $x^{-1} \in K$, and we have shown that $x^{-1} \in K$ whenever $x \in K$. That is, (SG3) holds.

Since K satisfies (SG1), (SG2) and (SG3), it is a subgroup of G.

For the last part, we must show that the subset I of H satisfies SG1, SG2 and SG3. For SG1, let a, $b \in I$. Then $a = \phi(x)$ and $b = \phi(y)$ for some x, $y \in G$, and so

$$ab = \phi(x)\phi(y) = \phi(xy).$$

This shows that $ab \in I$, since ab is obtained by applying ϕ to some element of G (namely, the element xy). Thus I is closed under multiplication: SG1 holds.

Since $e_H = \phi(e_G)$, we have that $e_H \in I$. So I satisfies SG2.

Let $a \in I$. Then $a = \phi(x)$ for some $x \in G$, and so

$$a^{-1} = \phi(x)^{-1} = \phi(x^{-1}) \in I.$$

Hence $a^{-1} \in I$ whenever $a \in I$; that is, SG3 holds. □