Math 417 Group Theory Miderm Exam
Things we have talked about so far

Symmetries: Group theory had its origins in the study of symmetry = a bijective (= injective and surjective) function $f : X \to X$ that preserves some chosen "structure". E.g., if structure = nothing, then f is 'just' a bijection (= *permutation*). If X is a vector space, then 'structure' might be vector addition and scalar multiplication (i.e., $f(\vec{v}+\vec{w}) = f(\vec{v}) + f(\vec{w})$), $f(c\vec{v}) = cf(\vec{v})$), and f is a (bijective) *linear transformation.* If X is a polygon/polyhedron, and f is a rigid motion (distance between points is preserved) which carries X to itself, then f is an *isometry* of X. If we wish to preserve both the vector space structure on $\mathbb{R}^n$ <u>and</u> the lengths of vectors, we get the collection of orthogonal $n \times n$ matrices (which are those which satisfy $A^TA = I$; the columns of A form an orthonormal basis).

An isometry which leaves the origin fixed is a linear transformation, and so is represented as multiplication by a matrix; for the plane, this means we have either a rotation by angle θ, R_θ or a reflection in an line with angle θ, M_θ, where

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \text{ and } M_\theta = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}$$

These are, in fact, the set of all symmetries of a circle centered at the origin. If we instead wish to look at the symmetries of a polygon P, then since a rigid motion must take the center of mass of (the region inside of) P to itself, they must all be rotations and reflections around that point, and must, in addition, take the vertices of P to vertices of P. This reduces the problem of finding all symmetries to a 'finite problem': which rotations/reflections preserve the vertices? For a regular n-gon, there are $2n$ of them; n rotations (including the identity map) and n reflections.

Symmetries are functions, and so can be composed; and the composition of two bijections that preserve a structure (like those above) is also a bijection that preserves the structure. So symmetries can be composed, and inverted, and the identity is a symmetry. This provides the model for our main object of study: groups.

Groups: Ultimately, the notion of a group can be introduced anywhere that 'objects/functions' can be both <u>composed</u> and <u>reversed</u>. The key obervation is that function composition is associative.

A group is any collection G of elements, together with a way to ('compose' =) multiply them, $G \times G \to G$, $(g, h) \mapsto g * h$ so that:

there is an 'identity': $e \in G$ so that $e * g = g * e = g$ for all $g \in G$

there are inverses: each $g \in G$ has a $g^{-1} \in G$ so that $g * g^{-1} = g^{-1} * g = e$

multiplication is *associative*: for all $g, h, k \in G$, we have $(g * h) * k = g * (h * k)$

A key property that is implicit in the definition of a group is *closure*: the product of two elements of G must again be an element of G.

Examples:

For small enough examples, we can represent the group multiplication by a *Cayley table*; a matrix which lists every multiplication. $g * h$ is listed in the g-th row and h-th column.

R = any ring (like $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) is a group when we consider only the adddition; $(\mathbb{Z}, +, 0)$. $+$ is the group operation, and 0 is the identity.

For F any field, the set $(F^*, \cdot, 1)$, where F^* is the set of non-zero elements, is a group under multiplication. Positive rationals, and positive reals, are also a group under multiplication.

$(\mathbb{Z}_n, +, 0)$, the integers modulo n, form a group under addition. $(\mathbb{Z}_n^*, \cdot, 1)$, the elements of $k \in \mathbb{Z}_n$ with k and n relatively prime, form a group under under multiplication; this is the group of *units* modulo n. This is because the Euclidean algorithm shows us that the product of two numbers a, b relatively prime to n is again relatively prime to n. That is:

$ak_1 + n\ell_1 = 1$ and $bk_2 + n\ell_2 = 1$ implies that $(ab)(k_1k_2) + n(\ell_1bk_2 + \ell_2ak_1 + n\ell_1\ell_2) = 1$

and because the gcd of two numbers m, n is both the largest integer that divides both m and n ($k|n$ and $k|m$ and no number larger than k does) and the smallest positive integer that can be expressed as $nx + my$ for integers x, y.

Alternate structures! $G = \mathbb{Z}$, with the multiplication $a * b = a + b = 7$, is a group; the identity element is -7 (!).

$\mathbb{Z}_{13}^*$, with multiplication $a * b = 3ab \pmod{13}$, is a group. The identity element is 9 (!).

Matrix groups: The set of invertible $n \times n$ matrices, with coefficients in any ring R, form a group. The group operation is matrix multiplication, the identity element is the identity matrix, and inverse are, well, inverses. Via the usual augmented matrix approach to inversion, or Cramer's Rule, the invertible matrices are precisely those matrices A whose determinant $\det(A)$ is a *unit* in R, i.e., has a multiplicative inverse. The invertible matrices over R are usually denoted $GL(n, R)$ or $GL_n(R)$, and is called the *general linear group.*

If we look at the cartesan product $\mathbb{Z}_n \times \mathbb{Z}_n^*$ of the integers modulo n with their group of units, we can define a product on these by $(a, b)(c, d) = (a + bc, bd)$. The identity element is $(0, 1)$, $(a, b)^{-1} = (-ab^{-1}, b^{-1})$, and multiplication is associative!

The symmetries of a polygon, or other geometrical figure P (that is, the rigid motions α with $\alpha(P) = P$, form a group under function composition, usually called the *isometry group of P*.

The set of affine functions $f(x) = mx + b$ (with $m \neq 0$) form a group under function composition.

The set of continuous functions $f : [0, 1] \to [0, 1]$ that are bijective form a group under composition; the Inverse Function Theorem implies that the inverse function f^{-1} is also continuous.

Some basic results that hold for any group:

The identity element is unique: if $xg = g = gx$ for every g, then $x = e_G$.

Inverses are unique: if $xg = gx = e_G$, then $x = g^{-1}$.

Cancellation Law: if $ac = bc$ then $a = b$, and of $ca = cb$ then $a = b$.

Inverse of a product: $(ab)^{-1} = b^{-1}a^{-1}$.

The *order* $|G|$ of a group G is the number of elements in the group.

Cancellation implies that the Cayley table of a group is a *latin square*: every group element appears exactly once in each row and column. [This is, however, not enough to guarantee associativity, evven when the multiplication is commutative...]

If the group multiplication is commutative - i.e., $ab = ba$ for every $a, b \in G$ - then we say that G is *abelian.* 'Most' groups are not abelian: general linear groups (when $n \geq 2$) are not, the groups $\mathbb{Z}_n \times \mathbb{Z}_n^*$ are (usually) not, and most isometry groups (e.g., for regular n-gons with $n \geq 3$) are not abelian.

If G is a group and $g \in G$, and $n \in \mathbb{Z}$, then we adopt the familiar exponential notation

$$g^n = g \cdot \cdots \cdot g \ (n\ g\text{'s}) \text{ if } n > 0$$
$$g^n = g^{-1} \cdot \cdots \cdot g^{-1} \ (|n|\ g\text{'s}) \text{ if } n < 0$$

and we define $g^0 = 1_G$

Then we have $g^{n+m} = g^n \cdot g^m$ and $g^{nm} = (g^n)^m$ for every $n, m \in \mathbb{Z}$. (This implies that the suggestive notation g^{-1} behaves the way it is supposed to.)

If G is finite, then for any $g \in G$ the powers g^n will eventually repeat themselves. When they first do, we have $g^n = e_G$. The order of g, $|g| = \min\{n \in \mathbb{N} \ : \ g^n = e_G\}$, satisfies: if $g^k = e_G$, then $|g|$ divides k.

Subgroups: There were several instances in which we 'borrowed' the group multiplication from one group so show that another set forms a group, e.g., $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \ : \ \det(A) = 1\} \subseteq GL_n(\mathbb{R})$ under matrix multiplication. This is a very common situation: we show something is a group by stealing the proof of the associativity of the group operation from another group.

A subset $H \subseteq G$ of a group G is a *subgroup* of G if, using the group operation from G, H is also a group. This amounts to showing three things:

If $a, b \in H$, then $ab \in H$ (closure)
$e_G \in H$, and
if $a \in H$, then $a^{-1} \in H$ (the inverse that lives in G actually lives in H)

The point is that, being a group, H must contain an inverse for $a \in H$, but since the group operation comes from G, this inverse must be the inverse a^{-1} that lives in G !

Examples:

$3\mathbb{Z} = \{3z \ : \ z \in \mathbb{Z}\} \subseteq \mathbb{Z}$ is a subgroup.

The set of diagonal matrices in $GL_n(\mathbb{R})$, and the set of upper triangular matrices, are both subgroups of $GL_n(\mathbb{R})$.

A one-step subgroup test: If $H \subseteq G$ and whenever $a, b \in H$ then $ab^{-1} \in H$, then H is a subgroup of G.

If H is finite, then $H \subseteq G$ is a subgroup if whenever $a, b \in H$ we have $ab \in H$. (This is because $a^n = e_G$ for some n, allowing us to establish that both e_G and inverses lie in H.)

More examples:

For $g \in G$, $\langle g \rangle = \{g^n \ : \ n \in \mathbb{Z}\}$ = the *cyclic subgroup* generated by $g \in G$. $|\langle g \rangle| = |g|$.

$Z(G) = C(G) = \{g \in G \ : \ gh = hg$ for every $h \in G\}$ = the *center* of G, is a subgroup of G.

[$Z(G) = \{e_G\}$ means that G is *centerless*.]

$Z_G(a) = C_G(a) = \{g \in G \ : \ ga = ag\}$ = the *centralizer* of a in G, is a subgroup of G.

If $H, K \subseteq G$ are subgroups of G, then $H \cap K$ is a subgrop of G. [Problem set!] This is also true for arbitrary intersections of subgroups.

Cyclic groups: G is *cyclic* if $G = \langle g \rangle$ for some $g \in G$.

If G is finite, then $G = \langle g \rangle \Leftrightarrow |G| = |g|$. So, for example, $\mathbb{Z}_{17}^* = \langle 10 \rangle$, so $\mathbb{Z}_{17}^*$ is cyclic. More generally, if p is prime, then it is a fact that $\mathbb{Z}_p^*$ is a cyclic group (although finding a generator can be rather challenging...)

Subgroups of cyclic groups: If $G = \langle g \rangle$ and $H \leq G$ is a subgroup, then $H = \langle g^k \rangle$, where k is the smallest (positive) exponent so that $g^k \in H$. Moreover, if $|g| = n$ is finite, then $k|n$ and $|H| = n/k$ also divides n. In general, if $|g| = n$ is finite, then $\langle g^k \rangle = \langle g^{\gcd(k,n)} \rangle$ (and $\gcd(k, n)$ gives the smallest power that lies in $\langle g^k \rangle$). This allows us to list all of the subgroups of a cyclic group $\langle g \rangle$.

In particular, if $G = \langle g \rangle$ is finite ($|g| = n$), then $\langle g^k \rangle = G \Leftrightarrow k$ and n are relatively prime. This implies that $\mathbb{Z}_n$ is cyclic with generator any integer relatively prime to n.

Permutations and permutation groups: for any set X, the set of bijections $f : X \to X$ form a group, $\mathrm{Perm}(X)$, under composition. For finite sets, we typically choose the set

$\{1, 2, \ldots, n\}$ (since it is the number of elements, and not their names, that really matter), and call the group S_n = the *symmetric group* on n elements. We can express an element by listing the images of 1 through n, in order, but we will ultimately find it (much) more conveient to use an alternate notation: cycles.

Cycle notation: The idea is that a cycle, like "(1364)", says '1 goes to 3, 3 goes to 6, 6 goes to 4, and 4 goes to 1', and every other number isn't moved.

Any element of S_n can be written as a product of cycles; just start at 1, and repeatedly write down where it goes (a, say), and then where a goes, repeating until we return to 1. Then pick something not listed in the cycle just written, and repeat the process. Continue until every number has been checked. No number will be written down twice, because that would mean that our bijection wasn't one-to-one. If a number k isn't moved, then part of our notation would include (k), but we omit it, and adopt the convention that any number not listed in a cycle is not moved by the cycle. This results in an expression for the permutation as a product of disjoint cycles (no two cycles share an element).

With this notation, function composition (the group operation) becomes concatenation, but a little care must be exercised. For example, if

$$f = (123) \text{ and } g = (12)(34) \text{ (all in } S_4)$$

then $f \circ g$ means g followed by f, i.e., $1 \to 2 \to 1$ and $3 \to 4 \to 3$, followed by $1 \to 2 \to 3 \to 1$
,

which is $1 \to 3 \to 4$, i.e., (134). The point is that we would write this as

$$(123)[(12)(34)] = (123)(12)(34)$$

but we must be careful how we read this; each individual cycle is read left to write, to determine where it sends each number, but the product of cycles must be read right to left, as function composition is done. For example,

$$(12453)(1423)$$

sends 1 to (4 to) 5, ***not** 1 to (2 to) 3. One way to think of it; each cycle has an arrow from left to right, to show how it is read, but the whole product has an arrow from right to left, to show how it is read.

Cylce notation has the advantage that a cycle like (123) can be thought of as sitting in S_3 or S_6 or any symmetric group S_n with $n \geq 3$, and the effects of multiplication will be the same in each of them. Another important point is that *disjoint cycles commute*; if α and β are two cycles that share no number in common, then $\alpha\beta = \beta\alpha$.

Having an expression for $\alpha \in S_n$ as a product of disjoint cycles also allows us to quickly determine the order $|\alpha|$; a cycle has order equal to its length, and so because the disjoint cycles commute, $|\alpha|$ is the least common multiple of the lengths of the disjoint cycles. And since ths calculation pays no attention to the contents of the cycles, just their lengths, we can determine the orders of every element of S_n by considering the ways to express n as a sum of positive integers (and the 1's that occur have no effect on the order).

Transpositions and parity: Every element of S_n can be expressed as a product of 2-cycles, since every k-cycle $(a_1, \ldots, a_k) = (a_1, a_2)(a_2, a_3) \cdots (a_{k-1}, a_k)$. [Alternatively, $(a_1, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2)$.] Even more:

Every expression of a given $\alpha \in S_n$ as a product of transpositions either always has an even number of 2-cycles (α is *even*) or always has an odd number of 2-cycles (α is *odd*).

This has many far-reaching consequences (essentially, anywhere where we wish to build an 'invariant' by counting/adding up large numbers of things, e.g., the determinant!). Of more immediate use to us is:

If we define a function sgn from S_n to $\{-1,1\}$ by sending even permutations to 1 and odd permuations to -1 (the 'sign' or 'signum' function), then $\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$. In particular, the product of two even permutations is even, and so the set A_n of even permutations on n letters is a subgroup of S_n (the *alternating group* on n letters). And since $\alpha \mapsto (1,2)\alpha$ sends even to odd and odd to even, we have $|A_n| = |S_n \setminus A_n|$ and so $|A_n| = (1/2)|S_n|$.

Homomorphisms and Isomorphisms: The set $\{-1,1\}$ forms a group under multiplication, and the signum map $\mathrm{sgn} : S_n \to \{-1,1\}$ send products to products; it is in some sense 'compatible' with the two group structures. This kind of 'structure-preserving' function (or 'map') between groups is a central topic of group theory.

A function $\varphi : G \to H$ from a group G to a group H is a *homomorphism* if for every $a, b \in G$ we have $\varphi(ab) = \varphi(a)\varphi(b)$. [Here the multiplication on the left takes place in G, while on the right it takes place in H.]

Such a map automatically has $\varphi(e_G) = e_H$, and $\varphi(a^{-1}) = [\varphi(a)]^{-1}$.

A homomorphism $\varphi : G \to H$ that is a bijection is called an *isomorphism.* [We then say that G and H are *isomorphic*, and write $G \cong H$.] The inverse φ^{-1} of an isomorphism in a homomorphism, and therefore is also an isomorphism. An isomorphism $\varphi : G \to G$ is called an *automorphism.* A homomorphism $\varphi : G \to G$ is called an *endomorphism.* An injective homomorphism is called a *monomorphism*; a surjective homomorphism is called an *epimorphism.*

Examples:

$\varphi : \mathbb{Z}_{16} \to \mathbb{Z}_{17}^*$, given by $\varphi(k) = 10^k \pmod{17}$, is an isomorphism.

$\det : GL_n(\mathbb{R}) \to \mathbb{R}$ is a homomorphism; $\det(AB) = \det(A)\det(B)$.

Conjugation: If $g \in G$, then $\varphi_g : G \to G$ given by $\varphi_g(x) = gxg^{-1}$ is an autmorphism. Its inverse is $\varphi_{g^{-1}}$. Such automorphisms are called *inner automorphisms.*

If $\varphi : G \to H$ is a homomorphism, then $|\varphi(g)|$ divides $|g|$.

If $\varphi : G \to H$ is an isomorphism, ,then $|\varphi(g)| = |g|$.

If $\varphi : G \to H$ is a homomorphism, then the *image* of φ, $\varphi(G) = \{\varphi(g) \ : \ g \in G\}$ is a subgroup of H. On the other hand, if φ is a homomorphism and $K \leq H$ is a subgroup of H, then $\varphi^{-1}(K) = \{g \in G \ : \ \varphi(g) \in K\}$, the *inverse image* of K, is a subgroup of G.

The composition of two homomorphisms is a homomorphism; the composition of two isomorphisms is an isomorphism. This means that $\mathrm{Aut}(G) = \{\varphi : G \to G \ : \ \varphi \text{ is an automorphism}\}$ is a group, the *automorphism group* of G, $\mathrm{Aut}(G)$.

Example: Every homomorphism $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ is $\varphi(x) = kx$ for some k [$k = \varphi(1)$], and so $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

If $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$, $\varphi(x) = kx$, is a homomorphism, then in order to be well-defined $m/\gcd(k,m)$ = the order of k in $\mathbb{Z}_m$ must divide n = the order of 1 in $\mathbb{Z}_n$.

If $G \cong H$, then:

$|G| = |H|$

If G is cyclic, then H is cyclic.

If G is abelian, then H is abelian.

Essentially, any property that can be described in terms of the group multiplication, which holds for G, must hold for H. ('Every element of G has order 2, 3, or 5', 'any element g which commutes with the square of another element h^2, must commute with h', 'every proper (i.e., not equal to G) subgroup of G is cyclic', etc.)

Cayley's Theorem: Every group G is isomorphic to a subgroup of a permuation group. Specifically, if $X = G$ (thought of as a set), then there is an injective homomorphism $\varphi : G \hookrightarrow \text{Perm}(X)$.

This homomorphism is given by $\varphi(g)(h) = gh$ (the 'left regular representation of G').

Homomorphism building: Orders of group elements can help us understand the existence/structure of homomorphisms.

A homomorphism $\varphi : S_3 \to \mathbb{Z}_3$ must send 2-cycles to (elements with order dividing 2, hence) the identity; but since every permutation is a product of 2-cycles (the 2-cycles 'generate' S_3), everything is sent to e.

A homomorphism $\varphi : S_5 \to S_4$ must send 5-cycles to e. But then products of 5-cycles, like $(1,2,3,4,5)(1,2,3,5,4) = (1,3)(2,4)$ go to the identity, so $\varphi(1,2) = \varphi(3,4)$. This leads to: the image of φ is cyclic, of order at most 2.

Cosets: The elements of $\mathbb{Z}_n$ can be thought of as *equivalence classes* of integers, with $a \equiv b$ if $n|b-a$. This can be interpreted as saying that $b-a$ lies in the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$. This perspective generalizes:

If $H \leq G$ is a subgroup of G, the the *left cosets* of H in G are the sets $aH = \{ah \ : \ h \in H\}$, and the *right cosets* of H in G are the sets $Ha = \{ha \ : \ h \in H\}$. Some basic properties:

$b \in aH \Leftrightarrow b = ah$ for some $h \in H \Leftrightarrow a^{-1}b = h \in H \Leftrightarrow b^{-1}a \in H \Leftrightarrow a \in bH$

$b \in Ha \Leftrightarrow ba^{-1} \in H \Leftrightarrow ab^{-1} \in H \Leftrightarrow a \in Hb$

For every $a, b \in G$ either $aH = bH$ or $aH \cap bH = \emptyset$

$h \mapsto ah$ gives a bijection $H \to aH$

If we choose one element a_i from each coset (these are *coset representatives*) then $a_1H, a_2H, \ldots$ partitions G into disjoint sets, each the same size as H. This gives:

Lagrange's Theorem: If H is a subgroup of G, then $|H|$ divides $|G|$.

Notation: $|G| = |H| \cdot [G : H]$, where $[G : H] =$ the number of (distinct) left cosets of H in G = the *index of H in G*. There is a argument completely parallel to the one we just gave, which uses <u>right</u> cosets Ha; so $[G : H]$ is <u>also</u> the number of right cosets of H in G.

An immediate consequence: for any $g \in G$, $|g| = | < g > |$ divides $|G|$.

This also gives *Euler's Theorem*: if $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$, since we can think $a \in \mathbb{Z}_n^*$, and $\varphi(n) = |\mathbb{Z}_n^*| =$ the number of integers $1, \ldots, n$ that are relatively prime to n (the 'Euler φ-function').

The map used to establish Cayley's Theorem (left-multiplication by a fixed element of G) can also be adapted to left-cosets of a subgroup H. If we let G/H denote the set of left cosets, then $\overline{\varphi}_g : G/H \to G/H$ given by $\overline{\varphi}_g(aH) = (ga)H$ is well-defined, and gives a permutation of the left-cosets of H. $\overline{\varphi}_g$ then defines a homomorphism $\overline{\varphi}(g) = \overline{\varphi}_g$ from G to $\text{Perm}(G/H)$. If $[G : H] = n$ is finite, then we can identify $\text{Perm}(G/H)$ with S_n by choosing a (fixed) bijection $\alpha : G/H \to \{1, \ldots, n\} = X$; then $\psi \in \text{Perm}(G/H)$ can be identified with $\alpha \circ \psi \circ \alpha^{-1} : X \to X$; the map $\psi \mapsto \alpha \circ \psi \circ \alpha^{-1}$ is an isomorphism. <u>Therefore</u>, a subgroup of G of index n 'induces' a homomorphism $\varphi : G \to S_n$, by the action of G on the left-cosets of H.

This kind of homomorphism-building occurs more generally. If X is an object with some kind of structure (think: the ideas we had at the start of the course!), then an *action* of a group G on X is a homomorphism $\varphi : G \to \text{Symm}(X)$; we say that G *acts on* X (via φ). The action is *faithful* if φ is injective; then G can be identified with a subgroup of the group of symmetries of X.

Going back to the action of G on left cosets, we get a homomorphism $G \to S_n$, but not just any homomorphism! Because left multiplication can take any coset aH to any other bH (the group element $g = ba^{-1}$ can do that), G acts *transitively* on the left cosets (G acts transitively on X if for any $x, y \in X$ there is a $g \in G$ with $g \cdot x = y$). We often supress the idea of a homomorphism into $\mathrm{Symm}(X)$, and write $g \cdot x$ for $\varphi(g)(x)$, to simplify the notation.

But in order to act transitively, we must have at least $[G : H]$ elements of $\varphi(G) \subseteq S_n$; we need that many elements to send $H = eH$ to all of the $[G : H]$ cosets of H. So the order of the image of G in S_n must be at least $[G : H]$. So, for example, our work understanding homomorphisms $\varphi : S_5 \to S_4$ means that S_5 has no subgroups of index 4 (since every homomorphism to S_4 has image of order at most 2).

Having an action of a group G on some object can help us to count things, like the order of the group itself! This is expressed by the Orbit-Stabilizer Theorem:

If $\varphi : G \to \mathrm{Symm}(X)$ is an action of G, and $x_0 \in X$, then the *stabilizer* of x_0 is $\mathrm{stab}_G(x_0) = \{g \in G \ : \ g \cdot x_0 = x_0\}$, the set of group elements which (thought of as symmetries of X) fix x_0. Because products (think: compositions!) of maps which fix x_0 also fix x_0, the stabilizer is a subgroup H of G. By Lagrange, then, $|G| = |H| \cdot [G : H]$, and so if we can determine both $|H|$ and $[G : H]$ then we can compute $|G|$. The point is that $[G : H]$ can be computed from the action; it is the size of the *orbit* $\mathrm{orb}_G(x_0) = \{g \cdot x_0 \ : \ g \in G\}$ of x_0 in X, the set of points that x_0 is sent to by the elements of G. This is because $a \cdot x_0 = b \cdot x_0 \Leftrightarrow (b^{-1}a) \cdot x_0 = x_0 \Leftrightarrow b^{-1}a \in \mathrm{stab}_G(x_0) = H \Leftrightarrow aH = bH$, and so the map $aH \mapsto a \cdot x_0$ is a bijection from the set of left cosets to the orbit of x_0. This gives:

Orbit-Stabilizer Theorem: If G acts on the set X, then for any $x_0 \in X$ we have $|G| = |\mathrm{stab}_G(x_0)| \cdot |\mathrm{orb}_G(x_0)|$.

This can be used to determine the order of G, identify subgroups $H = \mathrm{stab}_G(x_0)$ of G, and build (via the induced action of G on an orbit) homomorphisms/representations to symmetric groups $S_n \cong \mathrm{Perm}(\mathrm{orb}_G(x_0))$. For example:

$G = GL_2(\mathbb{Z}_{11})$ acts on the vector space $\mathbb{Z}_{11}^2$. If we set $x_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, then $Ax_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} x_0 = \begin{pmatrix} a \\ c \end{pmatrix} = x_0$ when $a = 1$ and $c = 0$, so $\det(A) = ad - bc = d \in \mathbb{Z}_{11}^*$ implies that $H = \mathrm{stab}_G(x_0) = \{\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \ : \ b \in \mathbb{Z}_{11} \text{ and } d \in \mathbb{Z}_{11}^*\}$, so $|H| = 11 \cdot (11 - 1) = 110$. On the other hand, $\mathrm{orb}_G(x_0) = \{\begin{pmatrix} a \\ c \end{pmatrix} \ : \ ad - bc \in \mathbb{Z}_{11}^* \text{ for some } b, d \in \mathbb{Z}_{11}\}$ essentially means that $(a, c) \neq (0, 0)$, and so $|\mathrm{orb}_G(x_0)| = 11^2 - 1 = 120$. So $|GL_2(\mathbb{Z}_{11})| = 110 \cdot 120 = 13200$.

Another example: The group G of rigid motions of a cube permute the vertices, the edges, and the (square) faces. In particular it permutes the centers of the square faces. If we pick one of them, x_0, then the orbit of x_0 is all of the centers of the squares, since we can construct rotations to send any one to any other. So $|\mathrm{orb}_G(x_0)| = 6$. Any motion which fixes x_0 sends the square face to itself, and so is 'really' a rigid motion of the square. Any such motion is induced from a rigid motion of the cube, and so $\mathrm{stab}_G(x_0)$ is (isomorphic to) the symmetries of the square, and so $|\mathrm{stab}_G(x_0)| = 8$. So $|G| = 6 \cdot 8 = 48$. Once know this, we can reverse direction: choosing x_0 to be a vertex of the cube, we can see that $|\mathrm{orb}_G(x_0)| = 8$ (all 8 vertices are in its orbit), and so $|\mathrm{stab}_G(x_0)| = 6$. [Check: the stabilizer is isomorphic to S_3 !]