Abstract Algebra. Math 6320. Bertram/Utah 2022-23.
Group Actions

Let X be a set and G be a group.

Definition. An *action* of G on X is a mapping:

$$\cdot : G \times X \to X$$

such that $e \cdot x = x$ for all $x \in X$, and $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $g_1, g_2 \in X$.

Proposition 1. An action of G on X is the same thing as a group homomorphism:

$$a : G \to \mathrm{Perm}(X)$$

Proof. For each $g \in G$, the mapping:

$$g\cdot : X \to X;\ x \mapsto g \cdot x$$

is a permutation (bijection) with inverse $g^{-1}\cdot$ since $g^{-1}\cdot(g\cdot x) = (g^{-1}g)\cdot x = e\cdot x = x$ and the conditions show that it is a group homomorphism. Conversely, given a group homomorphism $a : G \to \mathrm{Perm}(X),\ g \mapsto a_g$, let $g \cdot x = a_g(x)$. Then this is an action of G on X since $a_{g_1} \circ a_{g_2} = a_{g_1 g_2}$ and $a_e = 1_X$.

Examples. (a) Left and right multiplication (the latter by g^{-1}, as discussed earlier) are actions of G on itself.

(b) Conjugation is an action of G on itself that is also a map $c : G \to \ \mathrm{Aut}_{\mathcal{G}r}(G)$.

(c) Let $H \subset G$ be a subgroup. Then $c_g(H)$ is also a subgroup of G (by (b)), and conjugation determines an action:

$$c : G \to \mathrm{Perm}(\{H \subset G\})$$

on the set of subgroups of G.

(d) By definition, $\mathrm{GL}(n,k) = \ \mathrm{Aut}(k^n)$ in the category of vector spaces, so:

$$\mathrm{GL}(n,k) \times V \to V \text{ where } V = k^n$$

is an action of $\mathrm{GL}(n,k)$ on V. But invertible linear maps also take subspaces of k^n to subspaces of k^n (of the same dimension). Thus, if we let

$$\mathrm{Gr}(m,n)$$

be the "Grassmann" set of subspaces of k^n of dimension m, then we get an action:

$$\mathrm{GL}(n,k) \times\ \mathrm{Gr}(m,n) \to\ \mathrm{Gr}(m,n)$$

Remark. The Grassmannian $\mathrm{Gr}(m,n)$ is a projective variety of dimension $m(n-m)$, and if $k = \mathbb{R}$ or $\mathbb{C}$, then it is a compact manifold. Moreover, this action has more structure. It is "algebraic" in the sense of algebraic geometry.

Definition. (a) The *orbits* of an action $G \times X \to X$ are the sets:

$$Gx = \{gx \in X \mid g \in G\} \text{ for } x \in X$$

(b) The *stabilizer* of $x \in X$ given an action $G \times X \to X$ is the subgroup:

$$G_x = \{g \in G \mid gx = x\}$$

Proposition 2. Let G act on X and $x \in X$. Then there is a bijection:

$$\{gG_x |\ g \in G\} \longleftrightarrow Gx$$

between the left cosets of the stabilizer group of x and the points of the orbit of x.

Proof. The map from cosets to the orbit is $gG_x \mapsto g \cdot x$. This is

- Well-defined, since $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$ for all $h \in G_x$.
- Surjective (this is obvious), and
- Injective, since $g \cdot x = g' \cdot x$ if and only if $g^{-1} \cdot g' \in G_x$, i.e. $gG_x = g'G_x$.

Corollary. For $x \in X$ and an action of G on X, we have:

$$|G| = |G_x| \cdot |G/G_x| = |G_x| \cdot |Gx|$$

Examples. Conjugacy classes are the orbits of the conjugation action of G on itself (so $|Cl(h)|$ divides $|G|$ for finite groups), and if $H \subset G$ is a subgroup, then the orbits of the action of H on G by right multiplication are the left(!) cosets gH.

The Class Formula. For a finite group G acting on a finite set X,

$$|X| = \#\{\text{singleton orbits}\} + \sum_{|Gx_i|>1} |Gx_i| = \#\{\text{singleton orbits}\} + \sum |G|/|G_{x_i}|$$

where a representative x_i is chosen from each orbit. In particular,

$$|G| = |Z(G)| + \sum |\mathrm{Cl}(h_i)| = |Z(G)| + \sum |G|/|C_G(h_i)|$$

where we let $C_G(h) \subset G$ be the "centralizer" of h, i.e. the group of elements $g \in G$ that commute with h.

Proof. The first formula simply counts the elements of X by partitioning them into orbits under the action of G. The second formula is the special case of the action of G on itself by conjugation, for which $C_G(h)$ is the stabilizer of h. □

Recall that the order of $g \in G$ always divides $|G|$. We get a partial converse:

Cauchy's Theorem. If p is a *prime* dividing $|G|$, then some $g \in G$ has order p.

Proof. Suppose p divides $n = |G|$. Then by the class formula:

$$n = |Z(G)| + \sum |G|/|C_G(h_i)|$$

By induction on n, we may assume that p does not divide the order of any of the stabilizer subgroups $C_G(h_i) \subset G$, otherwise within $C_G(h_i)$ there would be an element of order p. Thus p divides each of the quotients $|G|/|C_G(h_i)|$.

But then p divides $|Z(G)|$, which is abelian, and by the classification of finite abelian groups, there must be an element of $Z(G) \subset G$ of order p. □

We may begin to classify some groups of various orders. Let p be a prime.

Corollary. (a) The only group with p elements is the cyclic group C_p.

(b) The only groups with p^2 elements are the cyclic group and $C_p \times C_p$.

Proof. (a) is immediate from Cauchy's Theorem.

For (b), it suffices to show that G is abelian. But:

$$p^2 = |Z(G)| + \sum |G|/|C_G(h_i)|$$

shows that $Z(G) \neq \{e\}$, and if $|Z(G)| = p$ (it has to divide p^2), then there is an element $h \notin Z(G)$ with $|\mathrm{C}_G(h)| = p$. But $Z(G) \subset C_G(h)$ (always) and $h \in C_G(h)$, which accounts already for $p + 1$ elements, giving a contadiction to $|Z(G)| = p$. Thus $|Z(G)| = p^2$, and G is abelian.

Example. This analysis does not extend to p^3, since, for example, the dihedral group D_8 of symmetries of the square is not abelian. It also does not extend to (all) groups of order pq for distinct primes p and q, since S_3 is not abelian.

We can, however, say something interesting about groups with p^d elements.

Definition. A group G with $|G| = p^d$ is called a *p-group*.

Definition. A group G is *solvable* there is a chain of subgroups:

$$0 = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_r = G$$

such that each H_i is normal in H_{i+1} and H_{i+1}/H_i is cyclic of prime order. Such a chain is called a *composition series* of the solvable group.

Remark. Solvable groups will be important in Galois Theory.

Examples. (a) All abelian groups are solvable (by the classification).

(b) The group S_3 is solvable, with series $0 \subset A_3 \subset S_3$.

(c) The group S_4 is solvable, with series $0 \subset C_2 \subset K_4 \subset A_4 \subset S_4$, where C_2 is any of the three cyclic subgroups of the Klein group.

(d) The *dihedral group* D_{2n} of symmetries of a regular n-gon is solvable via $C_n \subset D_{2n}$ the cyclic subgroup of rotational symmetries.

Proposition 3. Each p-group is solvable.

Proof. We prove more. As in the Corollary above, if H is a p-group, then:

$$|H| = p^d = |Z(H)| + \sum |H|/|C_G(h_i)|$$

shows that the center $Z(H)$ is a non-trivial abelian p-group, all of whose subgroups are therefore normal subgroups of G. Thus we can find a normal cyclic subgroup $C_p \subset H$. Then by the First Isomorphism Theorem, we get:

$$1 \to C_p \to H \xrightarrow{q} H/C_p \to 1$$

and then H/C_p contains a normal cyclic subgroup C_p' whose inverse image $q^{-1}C_p'$ is H_1, etc. In fact, each H_i in the composition series constructed in this way is a normal subgroup of H, and not just of H_{i+1}. This is "super"-solvable!

The p-groups are ubiquitous in group theory, because of the *Sylow Theorems*.

First Sylow Theorem. If $|G| = p^d m$ and $\gcd(m, p) = 1$, then there is a subgroup

$$H \subset G \text{ with } |H| = p^d \text{ (the maximal possible power of } p)$$

This subgroup H is called a *p-Sylow subgroup* of G.

Let S be the (non-empty) set of p-Sylow subgroups of G.

Second Sylow Theorem. The action of G on S by conjugation is *transitive*, i.e. it has only one orbit. Thus, in particular, $|S|$ divides $|G|$.

Let $H \subset G$ be a p-Sylow subgroup.

Third Sylow Theorem. The action of H on S by conjugation fixes H *and no other p-Sylow subgroup*. Thus, by the class formula,

$$|S| \equiv 1 \pmod{p}$$

and together with the Second Sylow Theorem, we conclude that $|S|$ divides m.

Proofs. The first Sylow theorem is a generalization of Cauchy's Theorem, and we prove it similarly, by induction on n. We start, as usual, with the class formula:

$$p^d m = |G| = |Z(G)| + \sum |G|/|C_G(h_i)|$$

First off, if p does not divide $|Z(G)|$, then p^d must divide one of the stabilizer subgroups $|C_G(h_i)|$ (otherwise p would divides all quotients $|G|/|C_G(h_i)|$, giving a contradiction). But then by induction on n, we know that $C_G(h_i)$ has a p-Sylow subgroup H with $|H| = p^d$, which is then also a p-Sylow subgroup of G.

If p does divide $|Z(G)|$, then by Cauchy's Theorem there is an element of the center $Z(G)$ of order p, hence a *normal* cyclic subgroup $C_p \subset Z(G) \subset G$. By the First Isomorphism Theorem, we obtain a quotient group:

$$q : G \to G/C_p \text{ of order } p^{d-1}m$$

which (by induction) has a p-Sylow subgroup $H \subset G/C_p$ with p^{d-1} elements. But then $q^{-1}(H) \subset G$ is a subgroup with p^d elements, i.e. a p-Sylow subgroup of G.

For the second theorem, we fix p-Sylow subgroups $H, H' \in S$ and consider the action of H on the set of left cosets $G/H' = \{gH'\}$ of H' by left multiplication. This set has size m, relatively prime to p, so by the class formula, it follows that there is a singleton orbit of the action (the size each orbit is a power of p). Thus, there is a left coset gH' such that:

$$h(gH') = gH' \text{ and so } (g^{-1}hg)H' = H' \text{ for all } h \in H, \text{ i.e. } g^{-1}Hg \subset H'$$

But H and H' have the same order, so $g^{-1}Hg = H'$ (and H' was arbitrarily chosen).

Finally for the third theorem, we fix a p-Sylow group H, and consider the action $H \to \text{Perm}(S)$ by conjugation. Then by the class formula,

$$|S| = \#\{\text{singleton orbits}\} + \sum |H|/|N_H(H_i)|$$

where $N_H(H_i) \subset H$ is the *normalizer* subgroup of elements h with $hH_ih^{-1} = H_i$. And since $|H| = p^d$, the size of every non-singleton orbit is divisible by p.

So it suffices to show that H is the *unique* Sylow subgroup normalized by H.

Suppose $H' \neq H$ is normalized by H and choose $h \in H$ outside of H'. Notice that as in the proof of the First Isomorphism Theorem, as a consequence of the fact that h normalizes H', we get:

$$hH' = H'h \text{ and so the left cosets } \{H', hH', h^2H', ..., h^{r-1}H'\}$$

are a cyclic group, with $h^r = h' \in H'$ (for r minimal). But the order of $h' \in H'$ is p^k for some k (since it divides $|H'|$), and likewise the order of h is p^l for some l, so $r = p^{l-k}$ is also a power of p, and the group generated by h and H':

$$\langle h, H' \rangle = \{h^i g \mid 0 \leq i \leq r-1,\ g \in H'\} \subset G$$

consists of $p^{l-k}|H|$ elements, which is a larger power of p, and a contradiction. □

As a numerical consequence, we get the existence of normal Sylow subgroups.

Corollary. If $|G| = p^d m$ with $m > 1$, and

$$a \not\equiv 1 \pmod{p}$$

for all factors a of m (other than 1), then the p-Sylow subgroup $H \subset G$ is normal.

Definition. A group G is *simple* if its only normal subgroups are $\{e\}$ and G.

Example. The cyclic groups C_p for primes p are the only simple abelian groups.

One might be forgiven for wondering whether there are any simple groups other than the cyclic groups of prime order. We will use the Sylow theorems and some cleverness to support this (wrong) hypothesis with some data:

All the simple groups of order $n < 60$ are cyclic. The p-groups are either of order p and cyclic or they are solvable (and not simple). Also, if $n = p^d m$ and $m < p$, then all divisors of m are smaller than p and so (except for 1) cannot be congruent to 1 mod p. So the p-Sylow subgroup is normal by the Corollary above. This leaves the following orders of groups that *might* be simple:

$$12, 24, 30, 36, 40, 45, 48, 56$$

Cancelling 40 and 45. This also follows directly from the Corollary above:

• $40 = 5 \cdot 8$ and $8, 4, 2 \not\equiv 1 \pmod 5$, so there is a normal 5-Sylow subgroup in every group with 40 elements.

• $45 = 5 \cdot 9$ and $9, 3 \not\equiv 1 \pmod 5$ and $45 = 3^2 \cdot 5$ and $5 \not\equiv 1 \pmod 3$ so there are a normal 5-Sylow subgroup *and* 3-Sylow subgroup in every group with 45 elements.

Cancelling $12, 30$ and 56. This follows from counting elements.

• $30 = 2 \cdot 3 \cdot 5$, so if G is simple and $|G| = 30$, then G has:

6 (cyclic) Sylow subgroups of order 5 accounting for $6 \times 4 + 1 = 25$ elements since they only overlap in the identity element.

10 (cyclic) Sylow subgroups of order 3, accounting for $10 \times 2 = 20$ more elements since the other divisors of 10 are 5 and 2, which are not congruent to 1 mod 3.

But $25 + 20 = 45 > 30$ is too many elements, so we have a contradiction.

• $12 = 3 \cdot 4 = 2^2 \cdot 3$, so if G is simple and $|G| = 12$, then G has:

4 (cyclic) Sylow subgroups of order 3, accounting for $4 \times 2 + 1 = 9$ elements.

3 Sylow subgroups of order 4, accounting for at least $3 + 1 = 4$ more elements.

This gives at least $9 + 4 = 13 > 12$ elements, and a contradiction.

Note that the alternating group A_4 has 4 Sylow subgroups of order 3 and the Klein subgroup K_4 as the unique Sylow subgroup with 4 elements.

• $56 = 7 \cdot 8 = 2^3 \cdot 7$, so if G is simple and $|G| = 56$, then G has:

8 (cyclic) Sylow subgroups with 7 elements, accounting for $8 \times 6 + 1 = 49$ elements.

7 Sylow subgroups with 8 elements, accounting for at least $7 + 1 = 8$ more.

And $49 + 8 = 57 > 56$.

Cancelling $24, 36$ and 48 by acting on a set of Sylow subgroups.

• $48 = 2^4 \cdot 3$, so if G is simple and $|G| = 48$, then G has three 2-Sylow subgroups, and conjugation acts non-trivially (in fact transitively) on the set S of these groups, which therefore defines a non-trivial group homomorphism: $a : G \to \mathrm{Perm}(S) = S_3$ But $|S_3| = 6 < 48$ so a cannot be injective, and the kernel is a normal subgroup!

• $36 = 3^2 \cdot 4$, so if $|G| = 36$ and G is simple, then there are four 3-Sylow subgroups. But then the conjugation action gives $G \to \mathrm{Perm}(S) = S_4$ and $36 > 4! = 24$ and the kernel is a normal subgroup.

• $24 = 3 \cdot 8 = 2^3 \cdot 3$ so if G is simple, then G has:

3 Sylow subgroups with 8 elements, and

4 Sylow subgroups with 3 elements (since $8, 2 \not\equiv 1 \pmod 3$).

Interestingly, the group S_4 does have this number of each. The Sylow subgroups with 8 elements are the three D_8 subgroups of S_4 and the Sylow subgroups with 3 elements correspond to the four ways to choose three elements from [4]. But in any case, letting S be the set of three Sylow subgroups with 8 elements, we get:

$$a : G \to \mathrm{Perm}(S) = S_3$$

giving a normal (non-Sylow!) subgroup of G. In the case $G = S_4$, this is our map onto S_3 (thinking of S_4 as the symmetries of the cube acting on short diagonals), and the kernel is the Klein four group, which we noted is normal in S_4.

When we pass to $|G| = 60$, none of these tricks work. If G is simple, there are:

6 (cyclic) Sylow subgroups with 5 elements, contributing $6 \times 4 + 1 = 25$ elements.

10 (cyclic) Sylow subgroups with 3 elements, contributing $10 \times 2 = 20$ more.

$15, 5$ or 3 Sylow subgroups with 4 elements. There can't be 3 by the last trick, since $3! < 60$, and 15 seems like too many, but there could certainly be five of them.

Looking at the alternating group A_5, we find indeed that it has:

6 Sylow subgroups with 5 elements, corresponding to the fact that there are exactly $24 = 4!$ elements of A_4 of order 5.

10 Sylow subgroups with 3 elements, corresponding to the fact that there are exactly $20 = \binom{5}{3} \times 2 = 20$ elements of A_4 of order 3

5 Klein subgroups coresponding to the 5 four element subsets of [5].

And indeed, A_5 is simple. In fact, we have:

Theorem. The alternating groups A_n are simple for all $n \geq 5$.

Before we tackle this, consider the conjugacy classes of A_n for small values of n. These are obviously related to the conjugacy classes of S_n. In fact,

Proposition 4. Let $N \subset G$ be a normal subgroup. Then for each $h \in N$,

$$|\mathrm{Cl}_N(h)| \text{ divides } |\mathrm{Cl}_G(h)| \text{ and } \frac{|\mathrm{Cl}_G(h)|}{|\mathrm{Cl}_N(h)|} \text{ divides } \frac{|G|}{|N|}$$

where $\mathrm{Cl}_N(h)$ is the conjugacy class of h in N.

Proof. By the orbit-stabilizer product formula, we have:

$$|N| = |\mathrm{Cl}_N(h)| \cdot |C_N(h)| \text{ and } |G| = |\mathrm{Cl}_G(h)| \cdot |C_G(h)|$$

and the centralizer groups satisfy: $C_N(h) = C_G(h) \cap N$, so we have:

$$\frac{|\mathrm{Cl}_G(h)|}{|\mathrm{Cl}_N(h)|} = \frac{|G|/|N|}{|C_G(h)|/|C_N(h)|} = \frac{|G|/|N|}{|C_G(h)|/|C_G(h) \cap N|}$$

and the result follows from the second isomorphism theorem for groups applied to the normal subgroup $N \subset G$ and the group $H = C_G(h)$.

Second Isomorphism Theorem. Let $H, N \subset G$ be subgroups with N normal. Then $H \cap N \subset H$ is normal, $HN = \{hn \mid h \in H, n \in N\} \subset G$ is a subgroup, and:

$$H/(H \cap N) \cong (HN)/N \subset G/N$$

Proof. (Exercise)

Applying the Proposition to $A_n \subset S_n$, we see if $h \in A_n$, then either:

$$|\mathrm{Cl}_{A_n}(h)| = |\mathrm{Cl}_{S_n}(h)| \text{ or else } 2|Cl_{A_n}(h)| = |Cl_{S_n}(h)|$$

i.e. either the conjugacy class is the same the one in S_n or it is half the size.

Conjugacy Classes in A_3, A_4, A_5 other than the trivial class $\{e\}$

$$A_3$$

This is cyclic, so $\{(1\ 2\ 3)\}$ and $\{(1\ 3\ 2)\}$ are conjugacy classes. We also knew that the conjugacy class of two elements for S_3 had to split in half because $|A_3| = 3$ and the size of a conjugacy class (for A_3) has to divide the order of the group!

$$A_4$$

The conjugacy classes of S_4 contained in A_4 are:

$$|\{(**)(**)\}| = 3 \text{ and } |\{(***)\}| = 8$$

The first can't split and the second has to because 8 does not divide $|A_4| = 12$. So there are four conjugacy classes in total, with $1, 3, 4, 4$ elements.

$$A_5$$

The conjugacy classes of S_5 contained in A_5 are:

$$|\{(**)(**)\}| = 15, |\{(***)\}| = 20 \text{ and } |\{(*****)\}| = 24$$

and keeping in mind that $|A_5| = 60$, we see that the first cannot split, the third must split, but the jury is out on the three-cycles. In fact, the class of three-cycles does **not** split, as we see below, but *even if it did*, we may conclude that the conjugacy classes of sizes $1, 15, 12, 12$ and 20 (or hypothetically 10 and 10) already show that:

A_5 **is simple.** A normal subgroup $N \subset A_5$ is a union of conjugacy classes including the identity class $\{e\}$. But none of the sums of sizes of conjugacy classes: $1+10, 1+12, 1+15, 1+10+10, 1+10+12, 1+12+12, 1+10+15, 1+12+15$ divides 60 (and all other sums are > 30). So there is not normal subgroup.

Next, as promised, we have a three-cycle interlude:

Proposition 5. (a) The class $\{(***)\} \subset S_n$ does not split in A_n when $n \geq 5$.

(b) Every element of A_n for $n \geq 3$ is a product of three-cycles.

Proof. (a) Given three-cycles $(a\ b\ c)$ and $(i\ j\ k)$, suppose $f \circ (a\ b\ c) \circ f^{-1} = (i\ j\ k)$. Then either $f \in A_n$ and there is nothing to do, or else $f \notin A_n$ is an odd permutation. But since $n \geq 5$, there is a two-cycle $(l\ m)$ that commutes with $(i\ j\ k)$, and replacing f with $(l\ m) \circ f$ also conjugates $(a\ b\ c)$ to $(i\ j\ k)$ and is an even permutation.

(b) The product $(a\ b\ c)(a\ b\ d) = (a\ c)(b\ d)$ shows that every product of a pair of disjoint two-cycles is in the subgroup generated by three-cycles. If $f \in A_n$, then f is a product of an even number of two-cycles. Grouping them in consecutive pairs, we see that each pair either annihilates each other, multiplies to a three-cycle or else is a pair of disjoint two-cycles (which we now see is a product of three-cycles). So f is a product of three-cycles. $\square$

We now prove the theorem by induction on n.:

Proof. (for $n \geq 6$). Suppose A_{n-1} is normal and $n \geq 6$. Let:

$$N \subset A_n \text{ be a normal subgroup}$$

Then as in the second isomorphism theorem, if we consider $A_{n-1} \subset A_n$, we have:

$$A_{n-1} \cap N \subset A_{n-1} \text{ is normal, and } A_{n-1}N \subset A_n \text{ is a subgroup}$$

Since A_{n-1} is simple (by assumption), $N \cap A_{n-1} \subset A_{n-1}$ is either:

(i) $N \cap A_{n-1} = \{e\}$, and then

$$|NA_{n-1}| = |N| \cdot |A_{n-1}| \text{ divides } |A_n|$$

Since $|A_n/A_{n-1}| = n$, it follows that $|N|$ divides n. It is easy to see, however, that when $n \geq 6$, all the (non-trivial) conjugacy classes in A_n have more than $n-1$ elements, and so $N = \{e\}$.

(Interestingly, this counting argument fails for $n = 4$, which is why the normality of A_3 does not imply that A_4 is normal. In fact, it feeds us the Klein conjugacy class with three elements and tells us that $A_3 \cdot K_4 = A_4$.)

(ii) $A_{n-1} \cap N = A_{n-1}$, so in particular, N contains a three-cycle, and then by Proposition 5(a), N contains **all** three-cycles, and by Proposition 5(b), $N = A_n$.

Thus the only normal subgroups of A_n are $\{e\}$ and A_n. That is, A_n is normal. $\square$

For Further Sleuthing. The next non-cyclic simple group after the alternating group A_5 (of order 60) is not A_6 (of order 360), but rather a group of order 168. This is a group of projective linear transformations over a finite field, and is itself part of another infinite collection of simple groups. If you are ambitious, you may try to prove that there are no simple groups of order $60 < n < 168$ other than the cyclic groups, but you will run into some sizes (e.g. $90, 112$ and 120), where our current bag of tricks is inadequate to the task!