Lecture 9-25: Group actions on sets

September 25, 2024

Welcome to graduate school (for the grad students) and to the course! Algebra is (in my unbiased opinion) one of the coolest subfields of mathematics; I am looking forward to exploring it with you. I will begin with group theory. Assuming you have seen the material through section 3.3 of the Dummit and Foote text, I will begin with group actions on sets (Chapter 4). Although everyone's background is different and some of you may have seen this material, I want to make sure we are all on the same page with it. As it happens, I had not seen this material myself when I started graduate school.

Throughout in my lecture notes all page references will be to the main text Dummit and Foote. I will provide such references whenever possible, but I will also cover some topics not included in that book. Let G be a group and A a set.

Definition, p. 41

We say that G *acts on* A if for every $g \in G, a \in A$ there is $g \cdot a \in A$ such that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a)$and $1 \cdot a = a$ for all $g_1, g_2 \in G, a \in A$; here 1 denotes the identity element of G.

More precisely, we say that G acts on A on the left in this case; if instead G acted on the right, we would write $a \cdot g$ for the action of $g \in G$ on $a \in A$ and would assume that $(a \cdot g_1) \cdot g_2 = a \cdot (g_1 g_2)$. Given a left action of G on A, we get a homomorphism π from G to S_A, the group of all permutations of A (bijections from A to itself) under composition; here $\pi(g)$ is the permutation sending $a \in A$ to $g \cdot a$. Conversely, given such a homomorphism π, we get a left action via the rule $g \cdot a = \pi(g)(a)$.

Definition, p. 112

If G acts on A and $a \in A$ then the *stabilizer* G_a (also denoted G^a) of a is the subgroup of $g \in G$ with $g \cdot a = a$. The *orbit* of a, denoted $G \cdot a$, is the subset $\{g \cdot a : g \in G\}$ of A. The action of G is *transitive* if the entire set A consists of just one orbit. The *kernel* of the action is the intersection $\cap_{a \in A} G_a$ of all stabilizers, or equivalently the kernel of the homomorphism from G to S_A. It is a normal subgroup of G, As an example, the dihedral group D_n of order $2n$, or the group of symmetries of a regular n-gon in the plane for $n \geq 3$, acts transitively on the vertices of the n-gon and on its edges. The stabilizer of a vertex consists of the identity and a single reflection about the line joining that vertex to the opposite one (if n is even) of the midpoint of the opposite side (if n is odd). The stabilizer of an edge likewise consists of the identity and a single reflection about the axis of symmetry passing through the midpoint of the edge.

In general, two of the most important examples occur when a group G acts on itself, or on a closely related set. In the *left multiplication* or *left translation* action, we set $g \cdot a = ga$ for $g, a \in G$, taking $A = G$. More generally, if H is a subgroup of G and G/H is the set of left cosets gH of H in G, we have an action of G on G/H defined by $g \cdot aH = gaH$. We also have the *conjugation* action of G on itself, defined by $g \cdot a = gag^{-1}$. The action of G on G/H is transitive; the stabilizer of a coset aH is the conjugate subgroup aHa^{-1} of H (see Theorem 3, p. 119).The conjugation action of G on itself, by contrast, is never transitive (unless G is trivial). Its orbits are called *conjugacy classes* (p. 123). The stabilizer of $a \in G$ with respect to this action is called the *centralizer* of a and is denoted $C_G(a)$.

In particular, any group G of order n is isomorphic to a subgroup of the nth symmetric group S_n (the group of permutations of an n-element set) (Cayley's Theorem), since the kernel of the left translation action is trivial. More generally, if $H < G$ is a subgroup of index n, then there is a homomorphism from G into S_n, corresponding to the left translation action on G/H. Its kernel is the intersection $\cap_{g \in G} gHg^{-1}$ of all conjugates of H in G. In particular, if the order $|G|$ of G fails to divide $n!$ then the action of G on G/H must have a nontrivial kernel, so that G has a nontrivial normal subgroup.

Any transitive action of a group on a set turns out to be isomorphic to the left translation action on cosets of a suitable subgroup. More precisely, if G acts on A and $a \in A$, then there is a bijection from the orbit $G \cdot a$ to the coset space G/G_a sending $g \cdot a$ to gG_a; this is indeed a bijection since $g_1 \cdot a = g_2 \cdot a$ if and only if $g_1 g_2^{-1} \cdot a = a$, or if and only if $g_1 G_a = g_2 G_a$. From Lagrange's Theorem (which I assume you have seen) we deduce the famous Orbit Formula (which scandalously is never stated in the text): if G is finite, acts on A, and $a \in A$, then $|G| = |G_a||G \cdot a|$; in words, the order of the group equals the order of any orbit of it times the order the stabilizer of any element of this orbit. We also see that the orbits of G on a set A do not overlap: any two orbits are either identical or disjoint.

As an interesting consequence, let G be finite and let H be a subgroup of index p, where p is the smallest prime number dividing $|G|$. Then H is necessarily normal in G (Corollary 5, p. 120). To see this observe that the homomorphism π from G into S_p arising from the action of G on G/H has image of order dividing $p!$. Since $|G|$ is not divisible by any prime less than p, but this image cannot be trivial (lest G fail to acts transitively on G/H) this image must have order exactly p. Then the order of G is p times the order of the kernel K of π, which in turn equals p times the order of H. But K is the intersection of all conjugates of H, so must be all of H, whence indeed H is normal in G, as claimed. (Note however that given G it may well be that no such subgroup H exists).

Now let G be a finite group acting on itself by conjugation. Conjugacy classes in G, being the orbits of G under the conjugation action, do not overlap and the union of all such classes is all of G. By the Orbit Formula and Lagrange's Theorem, the order of the conjugacy class of $g \in G$ equals the index $[G : C_G(g)]$ of the centralizer $C_G(g)$ of g in G. This order equals one if and only if $C_G(g) = G$, so that g lies in the center $Z(G)$ of G. We deduce

Theorem 7, p. 124; the class equation

We have $|G| = |Z(G)| + \sum_{i=1}^{s} [G : C_G(g_i)]$, where $g_1, \ldots g_s$ are representative of the conjugacy classes of noncentral elements of G.

The class equation is a particularly powerful tool for understanding *p-groups*; that is, finite groups whose order is a power of a prime p (see p. 139). We have

Theorem 1, p. 188

Let P be a p-group (for some prime p). Then

- The center $Z = Z(P)$ of P is nontrivial.
- Any proper normal subgroup H of P intersects Z nontrivially.
- P admits a chain of normal subgroups $P_0 \subset P_1 \subset \cdots \subset P_n = P$, where $|P_i| = p^i$.
- The normalizer $N_P(H)$ of any proper subgroup H of P strictly contains P.
- Any group of order p^2 is abelian.

Proof.

The terms $|Z|$ and $[P : C_P(p_i)]$ in the class equation of P are all powers of p; since $|Z| \geq 1$ and all indices $[P : C_P(p_i)]$ are multiples of p, $|Z|$ must also be a multiple of p, so that $Z \neq 1$. Any normal subgroup H of P is the disjoint union of its P-conjugacy classes; since one of these is the class of 1, the class equation again shows that $H \cap Z \neq 1$. In particular, since the order of any nonidentity element of Z is a power of p, Z must have an element z of order p. We now recall that for any group G and normal subgroup N there is a bijection between subgroups $\bar{H}$ of the quotient group G/N and subgroups H of G containing N, sending $\bar{H}$ to its preimage H under the canonical homomorphism from G onto G/N. □

Proof.

Applying this bijection to the normal subgroup N of P of order p generated by z and using induction, we get the desired chain of normal subgroups P_i. Likewise, given any proper subgroup H, either H contains N, in which case we can mod out by N and apply induction, or else H fails to contain N and N lies in its normalizer. Finally, if P has order p^2 and its center Z is not all of P, then choose $z \in P, z \notin Z$; then z commutes with itself and with Z, whence it commutes with all of P and lies in Z, a contradiction. □

Thus any p-group can be viewed as built up out of only one ingredient, namely the cyclic group of order p. Nevertheless, there is still a very rich theory of p-groups; for example, there are no fewer than 14 isomorphism classes of groups of order $16 = 2^4$.

In particular, any p-group G has the property admits a chain of subgroups $G_0 = 1 \subset \cdots \subset G_n = G$ such that each G_i is normal in G_{i+1} and the quotient G_{i+1}/G_i is cyclic of prime order. Groups with this last property are called solvable and will play a very important role in the theory of polynomials over a field, which I will develop next quarter. If in addition the G_i can be chosen so that G_{i+1}/G_i is central in G_n/G_i for all i, then one says that G is nilpotent. The above arguments show that any p-group is in fact nilpotent; it turns out that a finite group is nilpotent if and only if it is a direct product of p-groups (for various primes p).