6.857 R05: Groups

Andrew He

March 8, 2019

1 Groups

We'll begin by informally defining a group. A group is a generalization of an invertible associative binary operator, like "addition of reals", "matrix multiplication", or "multiplication mod p". A binary operator works on some particular elements (like "the reals", "invertible matrices", or "residues modulo p", for our examples above), so the set of elements it works on is an important part of the group.

Formally, we'll define a group $(G, \bullet)$ to be a set of elements G, together with some binary operator $\bullet$. (Think of $\bullet$ as a placeholder for whatever operator you're using.) The binary operator has a few requirements: (as you're reading these requirements, try checking them on the examples above)

- closed: for any two $g, h \in G$, $g \bullet h$ is also an element of G
- associative: $(g \bullet h) \bullet k = g \bullet (h \bullet k)$,
- has identity: there must be an element e such that $e \bullet g = g$ and $g \bullet e = g$.
- has inverses: for any $g \in G$, there's some element h such that $h \bullet g = g \bullet h = e$.

Because we're used to notation for addition and multiplication, we'll often "cheat" and write groups using $+$ or $\cdot$ as the operator. We'll actually sometimes go a step further and use "0" or "1" to denote the identity element (like in addition and multiplication), and we'll use $-g$ or g^{-1} to denote the inverse (like subtraction or division). Remember, these are just little cheats that help us because groups behave almost just like addition or multiplication to work.

2 Finite Groups and Generators

For a finite group, the number of elements of a group G is called the *order* of the group; we write it $|G|$ or $\text{ord}(G)$.

One useful way of analyzing a particular element of a group is by considering it's successive powers (both forwards and "backwards" by taking the inverse): in multiplicative notation, these would be

$$\{\ldots, g^{-2}, g^{-1}, g^0 = 1, g^1 = g, g^2, g^3, \ldots\} .$$

We'll call this set "the subgroup generated by g", and we'll sometimes write it as $\langle g \rangle$. The term "subgroup" means that it's a subset of the original group that's still a group with the same operation (you can check the requirements pretty easily).

In a finite group, there are only finitely many elements, so the subgroup $\langle g \rangle$ must also have finite size. That means that eventually, $g^k = 1$ again, and the group "cycles around". We call the size of $\langle g \rangle$ the *order* of g or $\text{ord}(g)$. We can note that $\langle g \rangle = \{1, g, \ldots, g^{\text{ord}(g)-1}\}$ and $g^{\text{ord}(g)} = 1$; otherwise, the subgroup group would be bigger or smaller.

Groups that look like $\{1, g, \ldots, g^{k-1}\}$ are called *cyclic groups*, because they're just a single cycle, and work as if we're adding the exponents modulo k. Note that $\langle g \rangle$ for any element is always cyclic.

An important theorem is that the order of an element g always divides the order of the group. (This is called *Lagrange's Theorem.*) This means that, if a group has prime order p, then the order of each element is either 1 or p; only the identity has order 1, so all other elements have order p, so $\langle g \rangle$ must equal to G for $g \neq 1$. Thus, any group of prime order is actually cyclic, and any non-identity element is a generator.

3 $\mathbb{Z}_p^*$ and Q_p^*

A useful group we'll use is $\mathbb{Z}_p^*$, the group of non-zero residues modulo p with multiplication. This has order $p - 1$, because we exclude 0.

It's a little tricky to show, but it turns out $\mathbb{Z}_p^*$ is actually a cyclic group of order $p - 1$! This means that $\mathbb{Z}_p^* = \{1, g, \ldots, g^{p-2}\}$ for some g. Furthermore, this means that g^2 has order $(p-1)/2$, as it generates the group $\langle g^2 \rangle = \{1, g^2, g^4, \ldots, g^{(p-3)}\}$ (every "even" element of $\langle g \rangle$). We call this group Q_p^*, which is the group of quadratic residues (perfect squares) modulo p.

If $p = 2q + 1$ is a safe prime, then Q_p^* has order q, which is prime, so it's cyclic. This is the basis for a lot of cryptography.