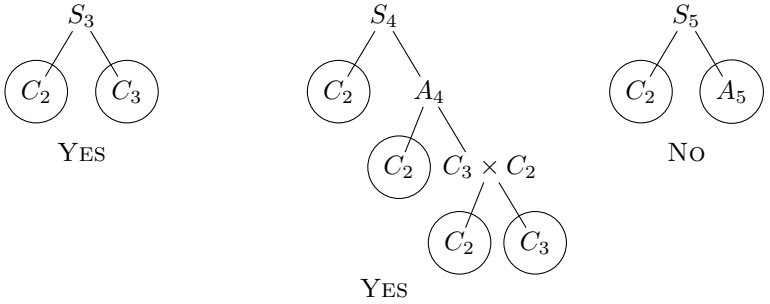
- The *symmetric group* S_n is the group consisting of all $n!$ ways to rearrange n objects. (The composition law is: do one rearrangement, then do another.) The *dihedral group* D_n is the geometric symmetries of a regular n-gon. The *cyclic group* C_n, also denoted $\mathbb{Z}/n\mathbb{Z}$, is just given by a single generator which comes back to the identity after it's performed n times, so you can think of it as the rotations of a regular n-gon. So we can see that for $n \geq 3$,
$$C_n \leq D_n \leq S_n.$$
- The *Galois group* is the group of "algebraic symmetries" of a polynomial. If the polynomial has degree n, then the Galois group must be a subgroup of S_n (because some but not necessarily all rearrangements of roots "preserve the structure" of the polynomial).
- A subgroup is called *normal* if it has some condition ($gng^{-1} \in N$ for all $n \in N, g \in G$) that guarantees that "you can divide by it" meaning that the quotient space G/N consisting of all the copies of N sitting inside G is itself a group. If N is a normal subgroup of G we write $N \trianglelefteq G$. In that case you can "factor" G into two smaller groups, N and G/N.
- A group is called *simple* if it has no normal subgroups other than $\{1\}$ and itself. (Just like a number is called *prime* if it has no integer factors other than 1 and itself.) The simple groups are the building blocks of all groups, in the sense that you can keep on factoring until all the pieces are simple, and then you can't continue.
- The *Jordan-Hölder theorem* says that for every group, any way of factoring it always produces the same list of simple factors! This should be thought of as "unique factorization for groups."
- **Galois's big insight** is that if a polynomial is solvable by radicals, then its Galois group factors into cyclic groups. He called such a group *solvable*.



Examples

Example 1. For the polynomial x^4-x^2-2, it factors completely into $(x-i)(x+i)(x-\sqrt{2})(x+\sqrt{2})$. The only nonidentity symmetries that preserve all algebraic relations between roots are swapping $\pm i$ and/or swapping $\pm\sqrt{2}$. If you count them up, that makes four possibilities in all (do nothing, do one swap, do the other swap, or do both).

Example 2. Consider x^3-2, which factors as $(x-\sqrt[3]{2})(x-\sqrt[3]{2}e^{2\pi i/3})(x-\sqrt[3]{2}e^{4\pi i/3})$. In this case, all ways of permuting the three roots are symmetries of the polynomial, so there are $3!=6$ symmetries in all.

Example 3. Next up is $x^4-2=(x-\sqrt[4]{2})(x-\sqrt[4]{2}\cdot i)(x+\sqrt[4]{2})(x+\sqrt[4]{2}\cdot i)$. Let's say $a=\sqrt[4]{2}$ so that the roots are $\pm a$ and $\pm ai$. Here are the symmetries:

- Do nothing.
- Switch $\pm a$.
- Switch $\pm ai$.
- Do both of the above swaps at the same time.
- Switch a with ai and simultaneously switch $-a$ with $-ai$.
- Switch a with $-ai$ and simultaneously switch $-a$ with ai.
- Send $a\mapsto ai\mapsto -a\mapsto -ai\mapsto a$.
- Same thing backwards! $a\mapsto -ai\mapsto -a\mapsto ai\mapsto a$.

Example 4. Finally, how about $x^{20}-1$? This has twenty roots, all arranged around the unit circle. If $b=e^{2\pi i/20}$, then the list of roots is $1,b,b^2,b^3,\ldots,b^{19}$. (That's a complete list of powers of b, because $b^{20}=1$ means the list starts over after that.)

Here is a full description of the symmetries. Let's suppose $f(b)=b^n$, and we take the rule that $f(b^k)=b^{kn}$. By this property, knowing where b goes completely determines where all of its powers go. (For example, the symmetry that sends $b\mapsto b^3$ also sends b^8 to $b^{24}=b^4$.)

There are exactly eight "algebraically rigid" symmetries of the roots, and those correspond to sending b to one of these: $b,b^3,b^7,b^9,b^{11},b^{13},b^{17},b^{19}$.

(A1) Suppose that the vertices of a regular octagon are labeled counterclockwise from 1 to 8. One example of a permutation of these that is in C_8 is the rotation

$$1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 6 \mapsto 7 \mapsto 8 \mapsto 1.$$

Give an example of a permutation of $\{1, \ldots, 8\}$ that is in S_8 but not D_8. Give an example in D_8 but not C_8.

(A2) For each of the four examples above, draw the roots in the complex plane. Consider the convex polygon formed by connecting the roots to each other in cyclic fashion.

For each, answer whether it is true or false that the algebraic symmetries described above are exactly the geometric symmetries (rigid motions) of the polygon in the picture. If it's true, explain what motion corresponds to what algebraic symmetry. If it's false, give an example of a geometric symmetry that's not an algebraic symmetry or vice versa.

(A3) For each of the four examples above, identify its Galois group using a name from the first page, or a product of those. (For instance, the Galois group of $x^3 - 1$ is C_2, as we discussed in class, because you can only switch two of the roots, but must leave the third one fixed.)

(B1) Up to isomorphism, there are exactly five different groups of order eight: (1) C_8, (2) $C_4 \times C_2$, (3) $C_2 \times C_2 \times C_2$, (4) D_4, and (5) Q. (Here, Q is the quaternion group consisting of $\{\pm 1, \pm i, \pm j, \pm k\}$ under quaternion multiplication.)
Which one of these is isomorphic to the Galois group of $x^{20} - 1$? Explain how you know!

(B2) An *abelian* group is one where every two elements commute: $ab = ba$ for all elements a, b. The *order* of a group is its number of elements. The *order* of an element is the number of times you have to do it to get back to the identity.

(a) Explain why every subgroup in an abelian group is normal.

(b) Suppose an abelian group of order n has an element whose order is less than n. Explain why the group is not simple.

(c) Using (b), prove that every abelian simple group is cyclic.

(d) Explain why the group C_{10} is not simple, but the group C_7 is.

(e) Putting everything together, give a complete classification of abelian simple groups.