Math 311 | Problem Set #7 | Due 1 November 2002

Reading: Gallian, Chapter 6.

Exercises: Write your solutions in complete sentences.

1. (Based on Chapter 6, exercise 11) Let G be a group, and for each $g \in G$, let φ_g denote the inner automorphism induced by g.

(a) Prove that $\varphi_g \varphi_h = \varphi_{gh}$ for all g and h in G.
(Recall that to show that two mappings φ_1 and φ_2 are equal, you let x be an arbitrary element of the domain and show that $\varphi_1(x) = \varphi_2(x)$.)

(b) Prove that the set of inner automorphisms of G forms a group under the operation of function composition. You may assume that function composition is associative. (This group is called $\mathrm{Inn}(G)$.)

2. (Based on Chapter 6, exercises 32, 33, and 34) Let G be a group. For each $g \in G$, let φ_g denote the inner automorphism induced by g. Prove that φ_g and φ_h are equal (as elements of $\mathrm{Inn}(G)$) if and only if $g^{-1}h \in Z(G)$, where $Z(G)$ denotes the center of G.

3. Let G be a group, and consider the mapping $\Phi : G \to \mathrm{Inn}(G)$ by

$$\Phi(g) = \varphi_g.$$

We already know that Φ preserves operations (that was problem 1a). Also, by construction, Φ is clearly onto. Prove that Φ is one-to-one (and therefore an isomorphism) if $G = S_3$, but that Φ is *not* an isomorphism if $G = D_4$.

4. (Based on Chapter 6, exercise 38) Consider the group $\mathbb{Z}_9$. For each $m \in U(9)$, the mapping $\alpha_m : \mathbb{Z}_9 \to \mathbb{Z}_9$ given by

$$\alpha_m(n) \quad = \quad mn \bmod 9$$

is an automorphism of $\mathbb{Z}_9$. (This fact is proved in the text.) That is, α_m permutes the elements of $\mathbb{Z}_9$, so we can view each α_m as an element of S_9.

(a) For each $m \in U(9)$, write α_m as a product of disjoint cycles.

(b) Recall that $U(9)$ is cyclic, and in fact $U(9) = \langle 2 \rangle$. Verify by direct calculation that $\alpha_{2^k} = (\alpha_2)^k$ for $k = 2$, 3, and 4.

5. (Optional) A set of permutations $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ is called a *set of generators* for S_n if any permutation in S_n can be written as a finite product of (positive and negative) powers of the α_i.

We already know that the set of all transpositions on the letters $\{1, 2, 3, \ldots, n\}$ is a set of generators for S_n, because any cycle, and thus any permutation, in S_n can be written as a product of transpositions. We also know that the set of all 3-cycles in S_n is *not* a set of generators, because any product of 3-cycles is an even permutation, and S_n always contains odd permutations (at least for $n > 1$).

Here's the challenge: let $\tau = (1\ 2)$ and $\sigma = (1\ 2\ 3\ \ldots\ n)$ be elements of S_n. Is the set $\{\tau, \sigma\}$ a generating set for S_n? Since we know that any permutation is S_n can be written as a product of transpositions, we can show that $\{\tau, \sigma\}$ is a generating set for S_n by giving a formula (or an algorithm) for writing an arbitrary transposition $(k\ l)$ in S_n as a product of powers of σ and τ. Try this.

Cultural aside:

He asked if Euler could find a proof. Euler could not, nor could anyone else, and so the statement "Every even integer greater than four is a sum of two odd primes" became known as the Goldbach conjecture. The Goldbach conjecture it will remain: even if Jane Doe, as a result of staggering ingenuity, hard work, and probably a little luck, proves that the conjecture is true, it will not go down in history as "Doe's Theorem." She will survive only in parentheses: what the books will say is, "Goldbach's conjecture, proved by Doe in 2032, states that ..." No matter what happens, the name of Goldbach is immortal.

It is not fair. *Anyone* can make conjectures. Conjectures are cheap. Goldbach also made one about odd integers: every odd integer, he conjectured, is the sum of a prime and twice a square. Just as with his other conjecture, it is true for small integers:

$$5 = 3 + 2 \cdot 1^2, \quad 7 = 5 + 2 \cdot 1^2, \quad 9 = 7 + 2 \cdot 1^2, \ldots,$$

but Goldbach's other conjecture fails at 5777, so his name is not attached to it. If a route to immortality is making conjectures, perhaps if you make enough of them you will be remembered for one. I may as well try: I conjecture that every composite odd integer is the sum of a prime, a square, and one or two cubes, as

$$9 = 3 + 2^2 + 1^3 + 1^3, \quad 15 = 5 + 3^2 + 1^3, \quad 21 = 3 + 4^2 + 1^3 + 1^3.$$

If that conjecture does not do the trick, more can be supplied.

Underwood Dudley, *Mathematical Cranks*