Abstract Algebra Exercises

Spencer T. Parkin

September 9, 2012

These problems are taken from Gallian's, "Contemporary Abstract Algebra."

Chapter 0

Exercise 7

Show that if a and b are positive integers, then $ab = \mathrm{lcm}(a, b)\,\mathrm{gcd}(a, b)$.

We first make the observation that if x and y are common multiples of a and b with $x < y$, then $x|y$. Therefore, if a given integer q is a common multiple a and b, we can show that it is the least such multiple if there is no integer k such that q/k is also a common multiple.

Letting $d = \mathrm{gcd}(a, b)$, we now make an argument that $\mathrm{lcm}(a, b) = ab/d$ by an examination of the prime factorization of ab/d. First, notice that ab/d is a common multiple of a and b, since we may write $a = da'$ and $b = db'$ and see that $ab/d = a'b'd$. To see that ab/d is the least common multiple of a and b, we notice that for an integer k such that $k|(ab/d)$, we must have $a \nmid (ab/(kd))$ or $b \nmid (ab/(kd))$, because division of ab/d by k must remove a non-redundant divisor of a or b appearing in the prime factorization of ab/d. Division of ab by d removes all redundant divisors of a and b in the prime factorization of ab.

This is not a very good proof, but it makes intuitive sense.

Exercise 10

Let $d = \mathrm{gcd}(a, b)$. If $a = da'$ and $b = db'$, show that $\mathrm{gcd}(a', b') = 1$.

Notice that if x is any common divisor of a and b, then $x|d$. Therefore, there are no non-trivial divisors of a/d and b/d. That is, division by d removes all non-trivial common divisors.

Exercise 13

Let n and a be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax \mod n = 1$ has a solution if and only if $d = 1$.

Noticing that $ax \mod n = (a \mod n)x \mod n$, we can assume, without loss of generality, that $0 < a < n$. Then...

Chapter 1

Exercise 5

For $n \geq 3$, describe the elements of D_n. How many elements does D_n have?

The group D_n, when $n \geq 3$, will have n rotation operations and n reflections operations. So the group will have order $2n$. The group D_2 has a 2 rotation and 2 reflection operations that are the same, so it must have order 2. The group D_1 has order 1.

Exercise 6

In D_n, explain geometrically why a reflection followed by a reflection must be a rotation.

Rotations preserve the winding order of the n-gon, but reflections do not. An even number of reflection will leave the winding order of the n-gon invariant. Then since the rotations are the set of all winding preserving operations, two successive reflections must be a rotation.

Exercise 7

In D_n, explain geometrically why a rotation followed by a rotation must be a rotation.

Because the set of all rotations in D_n forms its own sub-group.

Exercise 8

In D_n, explain geometrically why a rotation and a reflection taken together in either order must be a reflection.

An odd number of reflections combined with any number of rotations does not preserve winding order. The only non-winding-order-preserving operations are the reflections. So any rotation and reflection combination must be a reflection.