Chapter 7 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

February 14, 2014

Exercise 6

Let n be a positive integer. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$. Find all left cosets of H in Z. How many are there?

There are n of them. They are in $\{k + H\}_{k=0}^{n-1}$.

Exercise 8

Suppose that a has order 15. Find all of the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.

Since $|\langle a^5 \rangle| = 3$, there are $15/3 = 5$ such cosets. They are in $\{a^k H\}_{k=0}^{4}$.

Exercise 9

Let $|a| = 30$. How many left cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there. List them. By Theorem 4.2, we have $\langle a^4 \rangle = \langle a^2 \rangle$, which has order $30/2 = 15$. There are therefore $30/15 = 2$ left cosets, and they are $\langle a^4 \rangle$ and $a\langle a^4 \rangle$.

Exercise 10

Let a and b be nonidentity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.

Since $155 = 5 \cdot 31$, it is clear that the only possible orders of non-identity elements are 5, 31 and 155. If one of a and b has order 155, say $|a| = 155$, then clearly a is not in any one of the proper and non-trivial sub-groups, because 155 does not divide 5 or 31, so the result follows in this case. If a and b have orders less than 155, say $|a| = 5$ and $|b| = 31$, then a can be a subgroup of order 5, but not of 31, and b can be in a subgroup of order 31, but not of 5, because 5 does not divide 31, and 31 does not divide 5. The result goes through in this case too. We have now exhausted all cases.

Problem 12

Let C^* be the group of nonzero complex numbers under multiplication and let $H = \{a + bi \in C^* | a^2 + b^2 = 1\}$. Give a geometric description of the cosets of H.

Considering the polar form of complex numbers, it is easy to see that these are all possible concentric circles in the plane, centered at origin.

Problem 16

Recall that, for any integer n greater than 1, $\phi(n)$ denotes the number of integers less than n and relatively prime to n. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Notice that $a \in U(n)$ and that $|U(n)| = \phi(n)$. This result then follows directly from Corollary 4 of Legrange's Theorem.

Problem 18

Use Corollary 2 of Lagrange's Theorem to prove that the order of $U(n)$ is even when $n > 2$.

We must show that when $n > 2$, that $U(n)$ always has an element of order 2. Notice that $|n - 1| = 2$ for all $n > 2$.

problem 21

Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.

Notice that no element is its own inverse by Lagrange's Theorem, because 2 does not divide any odd number. Then, since making an element equivilant to its inverse produces an equivilance relation on a group, it partitions the group, and we can say that

$$e = \prod_{i=1}^{|G|} a_i a_i^{-1}$$

is a product of all the elemnts of G. Now notice that by the Abelian property of G, any rearrangement of this product is the identity.

Problem 22

Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)

This group is not the trivial group, so it has nonidentity elements. Consider the cyclic subgroup generated by any non-identity element. It is now clear that the group G is cyclic, because the cyclic subgroup just found cannot be proper. Furthermore, this cyclic subgroup must be of prime order, (and hence be finite), or else it would have nontrivial, proper subgroups by Theorem 4.3. (Notice that we did not need Lagrange's Theorem.)

Exercise 29

Let G be a group of permutations of a set S. Prove that the orbits of the members of S consitute a partition of S.

For any $a, b \in S$, let $a \sim b$ if and only if $a \in \text{orb}_G(b)$. To see that this forms an equivilance relation on the set S, we begin by noting that for all $a \in S$, we have $a \in \text{orb}_G(a)$, giving us the reflexive property. For all $a, b \in S$, if $a \sim b$, then $a \in \text{orb}_G(b)$ and therefore there exists $\phi \in G$ such that $\phi(b) = a$. Seeing that $\phi^{-1}(a) = b$ and $\phi^{-1} \in G$, it is clear that $b \in \text{orb}_g(a)$ and therefore $b \sim a$, giving us the symmetric property. Lastly, for all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, there exist $\phi_0, \phi_1 \in G$ such that $\phi_0(b) = a$ and $\phi_1(c) = b$. Then, letting $\phi = \phi_0\phi_1 \in G$, it is clear that $\phi(c) = a$ and therefore $a \in \text{orb}_G(c)$. It follows that $a \sim c$, and we have the transitive property.

Now notice that the equivilance class containing a is given by

$$[a] = \{x \in S | x \sim a\} = \{x \in S | x \in \mathrm{orb}_G(a)\} = \mathrm{orb}_G(a),$$

showing that the orbits of elements in S are the equivilance classes that partition S by Theorem 0.6.