Chapter 7 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

November 6, 2015

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 20

Suppose H and K are subgroups of a group G. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$.

The subgroup $H \cap K$ being that of H and K, the order of any element of $H \cap K$ must divide 12 and 35; but these are are relatively prime, so the order of all elements in $H \cap K$ is 1. The subgroup $H \cap K$ must therefore be the trivial subgroup having order 1.

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.)

Problem 23

Let $|G| = 15$. If G has only one subgroup of order 3 and only one of order 5, prove that G is cyclic. Generalize to $|G| = pq$, where p and q are prime.

By Corollary 3 of Legrange's Theorem, groups of prime order are cyclic. Therefore, G must have an element $a \in G$ of order p, and an element $b \in G$ of order q. Now choose $c \in G$ such that $c \notin \langle a \rangle$ and $c \notin \langle b \rangle$. (Such an element exists, because $G \neq \langle a \rangle \cup \langle b \rangle$ since $|G| > |a| + |b| - 1$.) Clearly c is not the identity element. Further, $|c|$ can't be p, otherwise there would exist more than one cyclic subgroup of order p. The order of c can't be q for a similar reason. Therefore, since $|c|$ must divide $|G| = pq$, it is clear that $|c| = |G|$, and we have $G = \langle c \rangle$.

Problem 24

Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all $g \in G$.

If G is cyclic, we're done. Suppose G is not cyclic. Then there does not exist $g \in G$ such that $|g| = 25$. The only possible orders for g are then, by Legrange's Theorem, one and five. The only element of order one is the identity, and clearly $e^5 = e$. It follows that $g^5 = e$ for all $g \in G$.

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

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

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

Problem 32

Prove that 3, 5, and 7 are the only three consecutive odd integers that are prime.

I'm not sure how to solve this problem in group-theory terms. Nevertheless...

Notice that $\{2k+1\}_{k=0}^{\infty}$ is the set of odd numbers. Now consider the subset of odd numbers $\{2(3k+1)+1\}_{k=0}^{\infty}$ and notice that every member is divisible by 3. But now also notice that one of every three consecutive odd numbers is in this subset.

Problem 33

Let G be a group of order p^n where p is prime. Prove that the center of G cannot have order p^{n-1}.

I have to use theorems in chapters yet to come to get this done. I'm not sure how else to do it.

Suppose $|Z(G)| = p^{n-1}$. Then, seeing that $Z(G)$ is always a normal subgroup of G, the factor group $G/Z(G)$ has order $p^n/p^{n-1} = p$, and is therefore cyclic. Therefore, there exists an element $g \in G$ such that $G/Z(G) = \{g^k Z(G) | k \in \mathbb{Z}\}$. Now since the cosets of $Z(G)$ cover G, if $a, b \in G$, there must exist integers $i, j \in \mathbb{Z}$ and elements $x, y \in Z(G)$ such that $a = g^i x$ and $b = g^j y$. It is then easy to see that $ab = ba$, showing that G is Abelian, and therefore $Z(G) = G$, but this contradicts the supposition that $Z(G)$ is a proper subgroup of G. It follows that $|Z(G)| \neq p^{n-1}$.

Now peaking at the back of the book, I see that a much easier proof exists.

Problem 36

Let G be a finite Abelian group and let n be a positive integer that is relatively prime to $|G|$. Show taht the mapping $a \to a^n$ is an automorphism of G.

Letting $\phi(x) = x^n$ be defined on G, it is clear that for all $x, y \in G$, we have $\phi(xy) = (xy)^n = x^n y^n = \phi(x)\phi(y)$ by the Abelian property of G, showing that ϕ is operation preserving.

Let $x, y \in G$ again and suppose that $\phi(x) = \phi(y)$. Then $x^n = y^n \implies e = x^n (y^n)^{-1} = (xy^{-1})^n$ by the Abelian property of G. Now since $(xy^{-1})^n = e$, we

see that $|xy^{-1}|$ divides n, (by Corollary 2 of Theorem 4.1), but it also divides $|G|$, (by Corollary 2 of Theorem 7.1.) Then since n and $|G|$ are coprime, it follows that $|xy^{-1}| = 1$, and therefore, $xy^{-1} = e \implies x = y$, and we see that ϕ is one-to-one. The function ϕ must then also be onto, because it is one-to-one and maps from one finite set to another of the same cardinality.

Problem 38

Let G be a group of order pqr, where p, q and r are distinct primes. If H and K are subgroups of G with $|H| = pq$ and $|K| = qr$, prove that $|H \cap K| = q$.

We know that $H \cap K$ is a subgroup of G. Let us first show that $H \cap K$ is not the trivial subgroup of G. Supposing this to be the case, we have...I don't know.

Let $g \in H \cap K$ be a non-identity element. Also being an element of H, we must have $|g|$ dividing pq. Being an element of K, we must have $|g|$ dividing qr. It follows that since $|g| > 1$, we must have $|g| = q$. Then, since all non-identity elements of $H \cap K$ have order q, it follows that $H \cap K$ is cyclic of order q.

Problem 45

If G is a finite group with fewer than 100 elements and G has subgroups of orders 10 and 25, what is the order of G?

The smallest possible order of G is $\text{lcm}(10, 25) = 50$. Any larger common multiple of 10 and 25 is at least 100. So $|G| = 50$.