Chapter 10 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

February 27, 2014

Lemma 1

Let H be a proper subgroup of G. Then for all $g \in G - H$ and all $h \in H$, $gh \in G - H$.

Suppose $gh = h' \in H$. Then $g = h'h^{-1} \in H$, which is a contradiction. Therefore, $gh \in G - H$.

Lemma 2

Let N be a normal subgroup of a group G. Then for any $g \in G$ and any $n \in N$, there exists $n' \in N$ such that $gn = n'g$ or such that $ng = gn'$.

Lemma 3

Let G be a group and let n be a positive integer. Then the number of elements in G of order n, if any, is divisible by $\phi(n)$, the totient of n.

Suppose G has one or more elements of order n. Let N be the set $\{x \in G||x| = n\}$. Then, for any pair of elements $a, b \in N$, let $a \sim b$ if and only if $a \in \langle b\rangle$. This defines an equivilance relation on N, since $a \in \langle a\rangle$ gives us the reflexive property, since $a \in \langle b\rangle \implies b \in \langle a\rangle$ gives us the symmetric property, and since $a \in \langle b\rangle$ and, for $c \in N$, $b \in \langle c\rangle$ implies that $a \in \langle c\rangle$, giving us the transitive property. We now note that by Theorem 4.4, the size of each equivilance class is $\phi(n)$. It follows that the number of elements of order n is G is $s\phi(n)$, where s is the number of equivilance classes.

Oh, I had already read this in the book as the Corollary to Theorem 4.4.

Exercise 38

For each pair of positive integers m and n, we can define a homomorphism from Z to $Z_m \oplus Z_n$ by $x \to (x \bmod m, x \bmod n)$. What is the kernel when $(m, n) = (3, 4)$? What is the kernel when $(m, n) = (6, 4)$? Generalize.

Let $\phi : Z \to Z_m \oplus Z_n$ be the homomorphism. Seeing that

$$\begin{aligned}\ker\phi &= \{x \in Z | x \equiv 0 \pmod m \text{ and } x \equiv 0 \pmod n\} \\ &= \{zm | z \in Z\} \cap \{zn | z \in Z\},\end{aligned}$$

it follows that

$$\ker\phi = \{z\operatorname{lcm}(m, n) | z \in Z\}.$$

Exercise 39

If K is a subgroup of G and N is a normal subgroup of G, prove that $K/(K \cap N)$ is isomorphic to KN/N.

Notice that the normality of the subgroup $K \cap N$ in K is proven by the problem similar to Exercise 50 in Chapter 9.

We now show that KN is a group. Let $x \in KN$. Then $x = kn$ for some $k \in K$ and $n \in N$. But then by Lemma 2 above, $x = n'k \in NK$ for some $n' \in N$. It follows that $KN \subseteq NK$. Similarly, we can show that $NK \subseteq KN$, so $NK = KN$. It then follows by Exercise 6 of the supplementary exercises for chapters 5 through 8 that NK is a group.

Is N normal in KN?

We now let $\phi : K/(K \cap N) \to KN/N$ be a function defined as

$$\phi(k(K \cap N)) = kN,$$

and show that it is a homomorphism. Let us first verify that this is a well defined function. Let $a, b \in K$ such that $a(K \cap N) = b(K \cap N)$. Then $ab^{-1} \in K \cap N \subseteq N$, showing that $aN = bN$.

We now show that ϕ is operation preserving. By the normality of N and $N \cap K$, we see that

$$\begin{aligned} &\phi(a(K \cap N)b(K \cap N)) \\ =&\phi(ab(K \cap N)) \\ =&abN = aNbN \\ =&\phi(a(K \cap N))(\phi(b(K \cap N)), \end{aligned}$$

showing that ϕ is operation preserving.

We now consider the kernel of ϕ. Notice that

$$\begin{aligned} \ker \phi &= \{k(K \cap N) \in K/(K \cap N) | k \in N\}, \\ &= \{k(K \cap N) \in K/(K \cap N) | k \in K \cap N\}, \\ &= \{K \cap N\}. \end{aligned}$$

It follows that ϕ is an isomorphism by Property 9 of Theorem 10.2.

Exercise 40

If M and N are normal subgroups of G and $N \leq M$, prove that $(G/N)/(M/N) \approx G/M$.

Notice that M/N is a subgroup of G/N. To see that M/N is normal in G/N, let $g \in G$ and let $m \in M$, and see that

$$gNmN(gN)^{-1} = gmNg^{-1}N = gmg^{-1}N \in M/N,$$

since $gmg^{-1} \in M$ by the normality of M in G.

Now consider the mapping $\phi : (G/N)/(M/N) \to G/M$, defined as

$$\phi(xN(M/N)) = yM,$$

where y is any element in the coset xN. Let us now show that this is a well defined mapping. Let $a, b \in G$ such that $aN(M/N) = bN(M/N)$. It follows that $aN(bN)^{-1} = ab^{-1}N \in M/N \implies ab^{-1} \in M$. Now let $aN(M/N)$ map to $a'M$ and $bN(M/N)$ map to $b'M$. Now if $a' \in aN \subseteq aM$, then $a'M = aM$. Similarly, if $b' \in bN \subseteq bM$, then $b'M = bM$. But now since $ab^{-1} \in M$, we see that $aM = bM$, so $a'M = b'M$.

Notice that the proof that ϕ is well defined also lets us simplify its usage. That is, for any $x \in G$, we can let $xN(M/N)$ map to xM. This will greatly ease the remainder of our proof.

We now show that ϕ is operation preserving. Letting $a, b \in G$, we have

$$\begin{aligned}
&\phi(aN(M/N)bN(M/N)) \\
=&\phi(aNbN(M/N)) \\
=&\phi(abN(M/N)) \\
=&abM = aMbM \\
=&\phi(aN(M/N))\phi(bN(M/N)).
\end{aligned}$$

We now consider the kernel of ϕ. We have

$$\begin{aligned}
\ker\phi &= \{gN(M/N) | g \in G \text{ and } \phi(gN) = M\} \\
&= \{gN(M/N) | g \in M\}.
\end{aligned}$$

Now let $a, b \in M$ and consider $aN(M/N)$ and $bN(M/N)$. Since $a, b \in M$, we have $ab^{-1}N \in M/N$, which, in turn, implies that $aN(bN)^{-1} \in M/N \implies aN(M/N) = bN(M/N)$. It follows that $|\ker\phi| = 1$, and therefore, ϕ is an isomorphism.

Exercise 47

Suppose that for each prime p, Z_p is the homomorphic image of a group G. What can we say about $|G|$? Give an example of such a group.

By Property 6 of Theorem 10.2, we see that $|\phi(G)|$ divides the order of $|G|$. So, since $\phi(G) = Z_p$, we see that p divides $|G|$.

An automorphism of Z_p may be a trivial example.

After reading the answer in the back of the book, I'm wrong, because I did not understand the problem statement. For *every* prime p, Z_p is *a* homomorphic image of *the* group G. So by Property 6 of Theorem 10.2, every prime p divides $|G|$; and since there are infinitely many primes, $|G| = \infty$.

Exercise 52

Let α and β be group homomorphisms from G to $\overline{G}$ and let $H = \{g \in G | \alpha(g) = \beta(g)\}$. Prove or disprove that H is a subgroup of G.

Clearly $e \in H$ by Property 1 of Theorem 10.1. Now let $a, b \in H$. We then have

$$\alpha(ab^{-1}) = \alpha(a)\alpha(b)^{-1} = \beta(a)\beta(b)^{-1} = \beta(ab^{-1}),$$

showing that $ab^{-1} \in H$. So I think it's a subgroup of G.