

# Chapters 5-8 Supplementary Exercises

## Gallian's Book on Abstract Algebra

Spencer T. Parkin

February 24, 2014

### Problem 1

A subgroup  $N$  of a group  $G$  is called a *characteristic subgroup* if  $\phi(N) = N$  for all automorphisms  $\phi$  of  $G$ . Prove that every subgroup of a cyclic group is characteristic.

Let  $\phi$  be an automorphism of  $G$ , a cyclic group. Let  $a$  be an element of  $G$ . Now see that

$$\phi(\langle a \rangle) = \{\phi(a^k) | k \in \mathbb{Z}\} = \{\phi^k(a) | k \in \mathbb{Z}\} = \langle \phi(a) \rangle.$$

Clearly,  $|a| = |\phi(a)|$ , so  $|\langle a \rangle| = |\langle \phi(a) \rangle|$ . We can now claim that  $\langle a \rangle = \langle \phi(a) \rangle$  by the fundamental theorem of cyclic groups, because  $G$  has one and only one subgroup of each possible order.

### Problem 2

Prove that the center of a group is characteristic.

Let  $\phi$  be any automorphism of a group  $G$ . If  $Z(G) = G$ , then  $Z(G)$  is trivially characteristic. So assume that  $Z(G)$  is a proper subgroup. Letting  $a$  be an element in  $\phi(Z(G))$  and  $g$  an element in  $G$ , there must exist an element  $a' \in Z(G)$  and an element  $g' \in G$  such that  $\phi(a') = a$  and  $\phi(g') = g$ . It then follows that

$$ag = \phi(a')\phi(g') = \phi(a'g') = \phi(g'a') = \phi(g')\phi(a') = ag,$$

showing that  $a \in Z(G)$ . Thus far we have shown that  $\phi(Z(G)) \subseteq Z(G)$ .

At this point, if  $Z(G)$  is finite, then we could argue that because  $\phi$  is one-to-one,  $\phi(Z(G))$  cannot be a proper subset of  $Z(G)$ , and therefore, we must have  $\phi(Z(G)) = Z(G)$ . But  $Z(G)$  may be infinite.

In any case, let  $z \in G$  such that  $\phi^{-1}(z) \in G - Z(G)$ . Suppose now that  $z \in Z(G)$ . Then for all  $g \in G$ , we have

$$\phi^{-1}(z)\phi^{-1}(g) = \phi^{-1}(zg) = \phi^{-1}(gz) = \phi^{-1}(g)\phi^{-1}(z),$$

showing that  $\phi^{-1}(z) \in Z(G)$ , (since  $\phi^{-1}$  is onto  $G$ ), which is a contradiction. Therefore,  $\phi^{-1}(z) \notin Z(G) \implies z \notin Z(G)$ . It follows that

$$z \in Z(G) \implies \phi^{-1}(z) \in Z(G) \implies z \in \phi(Z(G)),$$

and we have  $Z(G) \subseteq \phi(Z(G))$ .

## Problem 4

Prove that the property of being a characteristic subgroup is transitive. That is, if  $N$  is a characteristic subgroup of  $K$  and  $K$  is a characteristic subgroup of  $G$ , then  $N$  is a characteristic subgroup of  $G$ .

Let  $\phi \in \text{Aut}(G)$ . If  $\phi(K) = K$ , then  $\phi$ , when restricted in domain to  $K$ , is an automorphism of  $K$ . It follows that  $\phi(N) = N$ , showing that  $N$  is a characteristic subgroup of  $G$ .

## Problem 6

Let  $H$  and  $K$  be subgroups of a group  $G$  and let  $HK = \{hk | h \in H, k \in K\}$  and  $KH = \{kh | k \in K, h \in H\}$ . Prove that  $HK$  is a group if and only if  $HK = KH$ .

Suppose  $HK = KH$ . Clearly  $e \in HK$ . Let  $a, b \in HK$ . Then there exists  $h, h' \in H$  and  $k, k' \in K$  such that  $a = hk$  and  $b = h'k'$ , and we have

$$ab^{-1} = hk(h'k')^{-1} = hk(k')^{-1}(h')^{-1} = hh''k'' \in HK,$$

for some element  $h'' \in H$  and another  $k'' \in K$ , because  $HK = KH$ .

Now suppose  $HK$  is a subgroup of  $G$ . If  $a \in HK$ , then  $a^{-1} = hk$  for some  $h \in H$  and  $k \in K$ . It follows that  $a = k^{-1}h^{-1} \in KH$ . If  $a \in KH$ , then  $a = hk$  for some  $h \in H$  and  $k \in K$ . It follows that  $a^{-1} = h^{-1}k^{-1} \in HK \implies (a^{-1})^{-1} = a \in HK$ .

## Problem 7

Let  $H$  and  $K$  be subgroups of a finite group  $G$ . Prove that

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Consider the group  $H \oplus K$ , and define an equivalence relation on it as follows. For all  $a, b \in H \oplus K$ , let  $a \sim b$  if and only if  $a_h a_k = b_h b_k$ , where  $a = (a_h, a_k)$  and  $b = (b_h, b_k)$ . It is not hard to see that this is an equivalence relation on  $H \oplus K$  that partitions it into  $|HK|$  distinct equivalence classes. Now consider  $[(h, k)]$ , the equivalence class containing  $(h, k)$ . If  $(h', k') \in [(h, k)]$ , then  $hk = h'k' \implies (h')^{-1}h = k'k^{-1} = x \in H \cap K$ , showing that

$$[(h, k)] = \{(hx^{-1}, xk) | x \in H \cap K\}.$$

Furthermore, for any  $x, y \in H \cap K$ , if  $x \neq y$ , then  $(hx^{-1}, xk) \neq (hy^{-1}, yk)$ , showing that  $|[(h, k)]| = |H \cap K|$ . It now follows that

$$|H||K| = |H \oplus K| = |HK||H \cap K|.$$

## Problem 50

Suppose that  $H$  and  $K$  are subgroups of a group and that  $|H|$  and  $|K|$  are relatively prime. Show that  $H \cap K = \{e\}$ .

Let  $a \in H \cap K$ . Then  $|a|$  divides  $|H \cap K|$ , but since  $|H \cap K|$  divides  $|H|$  and  $|K|$ , we must have  $|a|$  dividing  $|H|$  and  $|K|$ . But if  $\gcd(|H|, |K|) = 1$ , then we must have  $|a| = 1 \implies a = e$ .