Outline of solutions to graded HW7

Shuai Wang

Exercise 2.9:

#5(b). It is easy to get the order of $G$ and $K$: $|G| = 24, |K| = 8$. So $|G/K| = \frac{|G|}{|K|} = 3$.

Note that this formula for the order is valid when $G$ is a finite group.

Whenever you use this formula, you have already assumed that $G$ is finite. If you get a problem by assuming $G$ is finite, you have done only a little part of it.

OK, let’s return to the problem. It is easy to know $K$ is a normal subgroup of $G$, so $G/K$ is a group. By Lagrange’s Theorem (it is a very important Theorem, remember it all the time), you get for the orders that

$|Ka^2|, |Ka^5|, |Kba^2| = 1$ or $3$. The remaining thing you need do is just to show $Ka^2 \neq K, Ka^5 \neq K, Kba^2 \neq K$, i.e., that the orders are all $3$.

Some of you made the following mistake: $a \in K \implies Ka \cdot a = Ka$. Maybe you are confusing this with the fact that $a \in K \implies Ka = K$, so $K$ seems to absorb every element which is in $K$. That is valid only for a subgroup $K$, not for a general coset $Ka$. You can see the nature of the mistake. If $Ka \cdot a = Ka$, then $Ka^2 = Ka$, so $a^{-1}a^2 = a \in K$, which is not the general $a \in G$.

#12. If $G/K$ has an element of order $n$, say $Kg$, then $(Kg)^n = K$. So $Kg^n = (Kg)^n = K, g^n \in K$. But $g^n$ is not necessarily equal to $1$, so we seem to be stuck.

How to proceed then? Since $G$ is finite, $g$ itself has an order. So let $|g| = m$, then $g^m = 1 \in K$. Thus $Kg^m = (Kg)^m = K$. For $|Kg| = n$ in $G/K$, it implies $n|m$. Let $m = dn$, then $1 = g^m = g^{dn} = (g^d)^n$. $g^d$ is the one of order $n$ in $G$. This statement is easy to prove, for $|g| = m$.

Maybe someone will wonder: why $|Kg| = n$ in $G/K$, and $(Kg)^m = K$, then $n|m$? It is due to the Division Algorithm, in section 1.2. (It is a very important theorem. Remember it if you do math.) Let $m = qn + r$, with $0 \leq r < n$. Then $K = (Kg)^m = (Kg)^{qn+r} = ((Kg)^n)^q(Kg)^r = K \cdot (Kg)^r = (Kg)^r$, so $r$ should be $0$, otherwise it would contradict $|Kg| = n$. So we have $m = qn$, i.e., $n|m$.

There are two meanings of order, and you need distinguish between them. One is the order of a group, which means the number of the elements in that group. The other is the order of an element $g$ in a group, which means equivalently the order of the subgroup generated by $g$, or the smallest positive exponent of that element needed to make it $1$. 

\#18. By a previous exercise (Exercise 2.6:\#31), this problem is pretty easy. Since \(|G : K| \text{ is finite, then by that exercise result, we know } |G : H| \text{ and } |H : K| \text{ are both finite, and } |G : K| = |G : H||H : K|. On the other hand, } G/K \text{ is a finite group, for } |G/K| = |G : K| \text{ is finite. So you can do what you usually do, for it is correct here: } |G/K : H/K| = \frac{|G/K|}{|H/K|}.

Combine these two equations, you can see easily how to get the answer.

Note: \(H/K\) is a subset of \(G/K\), for \(H/K = \{hK|h \in H\} \subseteq \{gK|g \in G\} = G/K\). Further you can show \(H/K\) is a subgroup of \(G/K\) easily.

Exercise 2.10:
\#8(b)(d). I wonder why one might not get this problem, because the Example 9 in the book tells you about it. OK, let’s do it.

(b). \(C_3 \rightarrow A_4\)

\(C_3\) has only two normal subgroups: \(\{1\}\) and \(C_3\). Thus if \(\alpha : C_3 \rightarrow A_4\) is a homomorphism, \(\ker\alpha\) must be one of them. If \(\ker\alpha = C_3\), \(\alpha\) is trivial. If \(\ker\alpha = \{1\}\), suppose \(C_3 = \langle g \rangle\), then \(\alpha(g)\) should have order 3 in \(A_4\). Just pick any element of order 3 in \(A_4\), you get a homomorphism. There are eight elements of order 3 in \(A_4\), so you have eight nontrivial homomorphisms.

(d). \(A_4 \rightarrow C_3\)

\(A_4\) has three normal subgroups: \(\{1\}\), \(K\) and \(A_4\), where

\[K = \{(12)(34), (13)24, (14)23, (1)\}\]

Thus if \(\alpha : A_4 \rightarrow C_3\) is a homomorphism, \(\ker\alpha\) must be one of them. It is impossible that \(\ker\alpha = \{1\}\) because then \(\alpha(A_4) \cong A_4\) would be a nonabelian subgroup of \(C_3\). If \(\ker\alpha = A_4\), then \(\alpha\) is the trivial homomorphism. So assume that \(\ker\alpha = K\). In this case let \(\varphi : A_4 \rightarrow A_4/K\) be the coset map. The Isomorphism Theorem guarantees that \(\alpha\) (if it exists) must be a composite \(\alpha = \sigma \varphi\), where \(\sigma : A_4/K \rightarrow \alpha(A_4)\) is an isomorphism. In this case, \(A_4/K = \{K, (123)K, (132)K\}\) is cyclic of order 3, so \(\alpha(A_4)\) is the (unique) subgroup of order 3 in \(C_3\), which is exactly \(C_3\) itself.

\(\sigma\) has two choices: \(\sigma((123)K) = g\) or \(g^2\), so for each choice, we have a nontrivial homomorphism \(\alpha\). You can write out the expression for \(\alpha\) respectively.

Note: To find out all the homomorphisms from a cyclic group \(\langle g \rangle\) to another group \(H\) is to find out all the possible images of the generator \(g\). For every possible image of \(g\), you have a corresponding homomorphism from \(\langle g \rangle\) to \(H\), and vice versa. Distinct possible images of \(g\) correspond to distinct homomorphisms. That’s cyclic group stuff, you can prove it yourself.

\#19. Let \(\varphi : G \rightarrow \mathbb{R}^*\), \(A \mapsto det(A)\); it is a surjective homomorphism. \(\ker \varphi = K\), so \(K < G\); and by Isomorphism Theorem, \(G/K \cong \mathbb{R}^*\).
#24. Let $\varphi : M_2(\mathbb{Z}) \rightarrow M_2(\mathbb{Z}_n)$, $A \mapsto \overline{A}$, every entry of $A$ goes to its residue class modulo $n$. It is a surjective homomorphism. $\ker \varphi = M_2(n\mathbb{Z})$, so $M_2(n\mathbb{Z}) \triangleleft M_2(\mathbb{Z})$, and by the Isomorphism Theorem, $M_2(\mathbb{Z})/M_2(n\mathbb{Z}) \cong M_2(\mathbb{Z}_n)$.