Outline of solutions to graded HW5

Shuai Wang

Exercise 2.5:

#6. Follow Example 9 in this section, and you can get easily that there are at most two homomorphisms \( C_6 \rightarrow C_4 \). A priori, there are three possibilities for the image (the three subgroups of \( C_4 \)), and two of the cases do occur, as you can check. [It may help for you to notice that \( C_6 \cong C_3 \times C_2 \).]

#12(d)(f). (d) Since \( G = G_1 \) are commutative groups, it is easy to check \( \alpha \) is a homomorphism. As for the bijectivity, just compute everything. \( \alpha(1) = 1, \alpha(2) = 3, \alpha(3) = 2, \alpha(4) = 4 \). Note that \( 0, 5 \notin G \).

(f) \( G \) and \( G_1 \) are additive groups now, while they were multiplicative groups in (d)(0 is in \( G = G_1 \), if they were multiplicative groups, what was the inverse of 0?). \( \alpha \) is a homomorphism but not surjective (1,3,5,7 don’t have preimages), so it is not an isomorphism.

#25. As an additive group, \( \mathbb{Z} \) is infinite cyclic while \( \mathbb{Q} \) is not. That is one’s intuition. To prove this problem, suppose that \( \alpha : \mathbb{Q} \rightarrow \mathbb{Z} \) is an isomorphism. Suppose the preimage of 1 is \( a \in \mathbb{Q} \), now consider \( a/2 \in \mathbb{Q} \), does it have image in \( \mathbb{Z} \) under \( \alpha \)? (If so, \( 2(a/2) \) maps to \( 1 \in \mathbb{Z} \).)

#37. (a) Reflexive: \( a \sim a \), for \( a = 1 \cdot a \cdot 1^{-1} \); here you can’t use some other \( g \in G \) instead of 1 because \( G \) is not assumed to be commutative.) Symmetric: If \( a \sim b \), then \( b = gag^{-1} \) for some \( g \in G \), thus \( a = g^{-1}bg = (g^{-1})b(g^{-1})^{-1} \), \( b \sim a \). Transitive: If \( a \sim b \) and \( b \sim c \), then write \( b = gag^{-1} \), \( c = hgh^{-1} \) for some \( g, h \in G \), thus \( c = hgh^{-1} = hgag^{-1}h^{-1} = (hg)a(hg)^{-1} \), so \( a \sim c \)(note here the elements \( g, h \) can not be presumed to be the same. The sentence “\( b = gag^{-1} \) for some \( g \in G \)” doesn’t mean \( g \) is a fixed element in \( G \). It just means there is some element in \( G \), denoted by \( g \). You must choose another symbol when the symbol \( g \) is already used.). After checking these three properties, we have by definition that \( \sim \) is an equivalence relation on \( G \).

(b) A singleton equivalence class is a class which has only one element. Of course, \( \{1\} \) is an example. In general, suppose \( \{a\} \) is a singleton equivalence class. It amounts to that \( \{a\} = \{b \in G | b \sim a\} \). And \( \{a\} = \{b \in G | b \sim a\} \iff \{a\} = \{b \in G | b = gag^{-1}, \text{for some } g \in G\} \iff \{a\} = \{gag^{-1}, \text{for all } g \in G\} \iff a = gag^{-1}, \text{for all } g \in G \iff a \in Z(G) \), the centralizer of \( G \). So, the elements of \( G \) that have singleton equivalence classes are exactly those in \( Z(G) \).
Exercise 2.6:

#12(a). $|G| = 12$, so by Lagrange’s Theorem, $|g|$ divides $|G|$. Thus the order of $g$ must be one of $1, 2, 3, 4, 6$ or $12$. If $|g| = 1, 2, 4$, then $g^1 = 1$; else if $|g| = 3, 6$, then $g^6 = 1$. They contradict the conditions given in the problem. So the only possibility is $|g| = 12$, which means $G = \langle g \rangle$.

#16. (a) Use the hint. $m$ and $n$ are relatively prime, then $1 = x m + y n$ for some integers $x$ and $y$. So $g = g^1 = g^{x \text{mod} y} = g^{x m} g^{y n} = (g^m)^x (g^n)^y = 1$ ($1^n = 1$ whenever $x$ is a positive or negative integer, or 0.)

(b) Use the hint. Let $\alpha : G \rightarrow G$, $a \mapsto a^m$ be a mapping. This problem requires you to show it is onto. So it suffices to show it is one-to-one by the hint. To show it is one-to-one, use the hint in (a). If $a^m = b^m$, then $a^{mx} = b^{mx}$, then $a = a^{mx-ny} = b^{mx-ny} = b$, for $a^m = b^m = 1$ ($|G| = n$, so $|a|, |b|$ divide $|G| = n$ by Lagrange’s Theorem). Note that $\alpha$ need not be a homomorphism, so you don’t show it is one-to-one by showing that the “kernel” is trivial ($a^m = 1 \implies a = 1.$)