Groups and Symmetry HW7 Solutions

November 7, 2014

Exercise 1. 11.2

Proof. Suppose $g_1H = g_2H$. Then $g_1 \cdot e \in g_1H = g_2H$ implies $g_1 = g_2h$ for some $h \in H$. Then $g_2^{-1}g_1 = h \in H$. Conversely, if $g_2^{-1}g_1 = h$ for some $h \in H$ then $g_1 = g_2h \in g_2H$, which implies g_1H and g_2H have a common element and thus are equal because the cosets form a partition. $\square$

Exercise 2. 11.3

Proof. If H and K are subgroups of G then their intersection $H \cap K$ is a subgroup of G and hence also of H and of K. Then the order of $H \cap K$ must divide both the order of H and the order of K, but these two numbers are relatively prime, so $\mid H \cap K \mid = 1$. Thus, H and K have only the identity element in common. $\square$

Exercise 3. 11.4

Proof. The order of any subgroup H must divide the order of the group $\mid G \mid = p \cdot q$ where p and q are distinct primes. Since H is proper, $\mid H \mid = 1, p$, or q and in each case H is cyclic by corollary 11.3 of the chapter. $\square$

Exercise 4. 11.5

Proof. This is similar to the proof of Lagrange's theorem. In this case, since we want the size of Y to divide the size of X, we will prove that the cosets of Y partition X. The set Y is finite so write it as $Y = \{e, y_2, y_3, \ldots, y_n\}$ (Y contains e because it is a subgroup). To begin select an $x_1 \in X$. Then $x_1Y = \{x_1, x_1y_2, \ldots, x_1y_n\} \subseteq X$ by assumption. If $x_1Y = X$ then Y and X have the same size, so certainly the size of X is a multiple of the size of Y. If not, then there exists and $x_2 \in X \setminus x_1Y$. We claim that x_1Y and x_2Y are disjoint. Suppose that they have a common element $x_1y_i = x_2y_j$. Then $x_1y_iy_j^{-1} = x_2$, which implies that $x_2 \in x_1Y$ and contradicts our choice of x_2. Thus, the two cosets are disjoint. If $X = x_1Y \cup x_2Y$ then $\mid X \mid = 2 \mid Y \mid$ and we are done. Otherwise choose a new element $x_3 \in X \setminus (x_1Y \cup x_2Y)$ and repeat the process. Since X is finite, this process will terminate, and X will be a disjoint union of cosets $x_1Y \cup \cdots \cup x_lY$. Thus, the size of X is a multiple of the size of Y. $\square$

Exercise 5. 11.7

Proof. As usual let s be a reflection element of D_n and r a rotation element by $2\pi/n$ of D_n. Suppose that m divides $2n$. There are two cases. If m divides n, then consider the element $r^{n/m}$. This element has order m, so generates a subgroup of order m. If m does not divide n evenly, then factor a 2 out of m and write it as $m = 2k$ (m must contain a factor of 2 because m divides $2n$). Then $2k$ divides $2n$ implies that k divides n. Consider the subgroup generated by s and $r^{n/k}$. The element $r^{n/k}$ has order k, so generates k elements $r^{n/k}, r^{2n/k}, \ldots, r^{(k-1)n/k}, r^{kn/k} = e$. Multiply each of these by s to get k more distinct elements $r^{n/k}s, r^{2n/k}s, \ldots, r^{(k-1)n/k}s, r^{kn/k}s = s$ (recall chapter on dihedral groups).

We still have to check that there is no other elements in the subgroup generated by $r^{n/k}$ and s. To this end recall the relation $sr = r^{n-1}s$ and let $z = n/k$ to ease notation. Then $r^{az}s \cdot r^{bz}s = r^{az}r^{(n-1)bz}ss = r^{(a+(n-1)b)z}$, which is an element in the set generated by r^z. Likewise, $r^{az}r^{bz}s = r^{(a+b)z}s$ is in the second set of elements listed above. Thus, these $m = 2k$ elements are indeed the distinct elements of this subgroup as desired. ☐

Exercise 6. 11.9

Proof. Consider the following claim. If a and b are elements of G of orders x and y respectively, then there is an element of order $lcm(x, y)$. If this claim is true, then the theorem is true because we can pick two elements g_1 and g_2 in G of orders o_1 and o_2 and get an element of order $m_1 = lcm(o_1, o_2)$. Then we can choose another element $g_3 \in G$ of order o_3. If $lcm(m_1, o_3) = m_1$ then continue on to the next step. Otherwise, the claim says that there exists an element of order $m_2 = lcm(m_1, o_3)$. Then pick $g_4 \in G$, and so forth. This process must terminate because G is a finite group.

To prove the claim, let $a, b \in G$ have orders x and y respectively and let $m = lcm(x, y)$. Then $(ab)^m = abab \cdots ab$ (m times) $= a^m b^m$ because G is abelian. Since x divides m and y divides m, $(ab)^m = a^m b^m = ee = e$. Therefore the order of ab must be at most m and must divide m. We would like to show that the order is actually equal to m.

Suppose first that x and y are relatively prime, so that $m = xy$. Let r be some number such that $0 < r < m$ and $(ab)^r = e$. Then $e = (ab)^r = a^r b^r$ implies that $a^{-1} = a^{r-1}b^r$. Since the order of a^{-1} is also x we have that

$$\begin{aligned} e &= (a^{-1})^x \\ &= (a^{r-1}b^r)^x \\ &= a^{x(r-1)}b^{(xr)} \\ &= eb^{xr} \\ &= b^{xr}. \end{aligned}$$

This means that the order of b divides xr, i.e. $y \mid xr$. But since x and y are relatively prime this means that y divides r, i.e. $yk = r$ for some k. Therefore, $b^r = b^{yk} = (b^y)^k = e$ and $e = a^r b^r = a^r$. From this we see that x also divides r, and since both x and y divide r, their least common multiple m must also divide r. Therefore, m is indeed the smallest integer such that $(ab)^m = 0$, so ab has order m.

Now suppose that x and y are not relatively prime, so that $g = \gcd(x, y) > 1$. Let $x' = x/g$, so that $a^{x/x'} = a^{x/(x/g)} = a^g$ has order x'. Then x' and y are relatively prime so by the previous part there exists an element of order $lcm(x', y) = x'y = \frac{xy}{g} = lcm(x, y)$ (recall $lcm(x, y)gcd(x, y) = xy$). □

Exercise 7. 11.10

Proof. Consider S_3 which has the identity of order 1, three elements of order 2, and two elements of order 3. Thus, the lcm of the orders is 6, but S_3 does not have an element of order 6 (if it did then that element would generate all of S_3 making it cyclic). □

Exercise 8. 12.1

Proof. (a) Yes, check the three axioms.
Note that 0 is even because 2 divides it.

(b) Yes, check the three axioms.

(c) No, fails transitivity.
Let $x = 1 + \sqrt{1}$, $y = -\sqrt{2}$ and $z = 2 + \sqrt{2}$. Then $x + y = 1$, $y + z = 2$, so x is related to y and y is related to z, but $x + z = 3 + 2\sqrt{2}$ is irrational so x is not related to z.

(d) No, $5 - 3 \geq 0$ but $3 - 5 < 0$, so fails symmetry.

□

Exercise 9. 12.3

Proof. Let G be S_3 and consider the subgroup $H = \{e, (12)\}$. Then $(123)(23) = (12) \in H$, but $(23)(123) = (13) \notin H$, so the relation fails symmetry. □

Exercise 10. 12.6

Proof. Let x and x' be two representatives of the same congruence class mod n. Then there exists a k such that $x = x' + kn$. Likewise, let $y = y' + ln$. Then $x + y = x' + kn + y' + ln = x' + y' + (k + l)n$, so $x + y$ and $x' + y'$ are congruent mod n and addition is well-defined. The identity in this group is $[0]$, the inverse of $[x]$ is $[-x]$, and the sum of two equivalence classes is an equivalence class mod n, so this set forms a group. Since addition is commutative, this is an abelian group. If we denote by $\mathbb{Z}'_n$ as the group defined on page 12 of the book, then $\phi : \mathbb{Z}'_n \to \mathbb{Z}_n$ defined by $\phi(x) = [x]$ is an isomorphism. It is bijective and $\phi(x + y) = [x + y] = [x] + [y] = \phi(x) + \phi(y)$. □