

ABSTRACT ALGEBRA A
HOMEWORK 3 SOLUTIONS

3-1. The elements of the j^{th} column will be

$$g_1g_j, g_2g_j, g_3g_j, \dots, g_i g_j, \dots$$

If two of these entries were equal, then we would have $g_n g_j = g_m g_j$ with $n \neq m$. Multiplying both side on the right by g_j^{-1} would then give

$$g_n = g_n e = g_n (g_j g_j^{-1}) = (g_n g_j) g_j^{-1} = (g_m g_j) g_j^{-1} = g_m (g_j g_j^{-1}) = g_m e = g_m,$$

a contradiction.

3-2. Every element $g_k \in G$ can be written in the form

$$g_k = g_k e = g_k (g_j^{-1} g_j) = (g_k g_j^{-1}) g_j.$$

Since the elements of the j^{th} column are exactly the elements of the form $x g_j$ for some $x \in G$, this shows that g_k appears in the j^{th} column.

3-14. Just work them out.

$$(134) = \begin{pmatrix} 1234 \\ 3241 \end{pmatrix}, \quad (12)(34) = \begin{pmatrix} 1234 \\ 2143 \end{pmatrix}, \quad (1423) = \begin{pmatrix} 1234 \\ 4312 \end{pmatrix},$$

$$(13)(12) = \begin{pmatrix} 1234 \\ 2314 \end{pmatrix}, \quad (14)(13)(12) = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix}.$$

3-17. We can actually do more than this. Suppose $\phi : (G, \cdot) \rightarrow (H, \star)$ is an homomorphism, and suppose e and i are the identities of G and H , resp. Then

$$\phi(e) = \phi(e \cdot e) = \phi(e) \star \phi(e).$$

Multiplying both sides by $\phi(e)^{-1}$ (Is this the inverse in G or in H ?) gives

$$i = \phi(e) \star \phi(e)^{-1} = (\phi(e) \star \phi(e)) \star \phi(e)^{-1} = \phi(e) \star (\phi(e) \star \phi(e)^{-1}) = \phi(e) \star i = \phi(e),$$

as desired.

3-18. Again, this holds for any homomorphism. With the same notation as in the previous problem, we have, for every $g \in G$,

$$\phi(g) \star \phi(g^{-1}) = \phi(g \cdot g^{-1}) = \phi(e) = i.$$

Since we have already proven that the inverse of every element of a group is unique, this implies that $\phi(g^{-1})$ is the inverse in H of $\phi(g)$, i.e., that $\phi(g^{-1}) = \phi(g)^{-1}$.

3-26. If both $g = t_1 t_2 \cdots t_{2k}$ and $h = s_1 s_2 \cdots s_{2m}$ are products of even numbers of transpositions, then $gh = (t_1 t_2 \cdots t_{2k})(s_1 s_2 \cdots s_{2m})$ is also a product of an even number $2(k + m)$ of transpositions. Further, since every transposition is its own inverse, $g^{-1} = t_{2k} t_{2k-1} \cdots t_1$ is also even. Thus, \mathcal{A}_n is closed under multiplication and under inverses; so by Theorem 3-6, it is a subgroup of \mathcal{S}_n .

- 3-27.** It's pretty easy to determine just by trial and error that the 4-group has exactly 5 subgroups:

$$\begin{aligned} &\{e\} \\ &\{e, a\} \\ &\{e, b\} \\ &\{e, c\} \\ &\{e, a, b, c\}. \end{aligned}$$

- 3-28.** This only requires being careful with each calculation about whether we are working in G or in H . Let i be the identity in H , and let e be the identity in G . Then

$$ii = i = ie,$$

where the first equality holds because i is the identity in H , and the second equality holds because e is the identity in G . Left-multiply both sides by the inverse of i in G , and you get

$$i = ei = (i^{-1}i)i = i^{-1}(ii) = i^{-1}(ie) = (i^{-1}i)e = ee = e;$$

so the conjecture is true.

- 3-29.** This one is also true. The inverse in H of h is an element $x \in H$ for which $hx = xh = i = e$. Since $x \in H \subseteq G$, this x also satisfies exactly the same conditions it would need to have in order to be the inverse of h in G ; so we're done.

- 3-31.** Right congruence is reflexive because for every $g \in G$, $g = eg$, and $e \in H$.

To show that right congruence is symmetric, suppose a is right congruent to b , i.e., that $a = hb$ for some $h \in H$. Then

$$b = (h^{-1}h)b = h^{-1}(hb) = h^{-1}a.$$

Since H is closed under inverses, $h^{-1} \in H$; so b is right congruent to a .

Finally, for transitivity, suppose that for a is right congruent to b and that b is right congruent to c . This means that there are elements h and k of H such that $a = hb$ and that $b = kc$. Substituting, we get $a = h(kc) = (hk)c$. Since H is closed under group multiplication, $hk \in H$; and a is right congruent to c . This completes the argument.

- 3-32.** The problem gives the central idea. Define a mapping η from left cosets to right cosets by $\eta(gH) = Hg^{-1}$. We need to show that η is a well-defined bijection.

First, to show that η is well-defined, suppose that $g_1H = g_2H$. This means that for some $h \in H$, $g_1 = g_2h$. From this, we get that

$$\eta(g_1H) = Hg_1^{-1} = H(g_2h)^{-1} = H(h^{-1}g_2^{-1}) = (Hh^{-1})g_2^{-1} = Hg_2^{-1} = \eta(g_2H),$$

proving that η is well-defined.

That η is surjective is easy. Any right coset $Hg = H(g^{-1})^{-1} = \eta(g^{-1}H)$ is in the image of η .

Finally, to show that η is injective, we begin by supposing that $\eta(g_1H) = \eta(g_2H)$, i.e., that $Hg_1^{-1} = Hg_2^{-1}$. This means that for some $h \in H$, $g_1^{-1} = eg_2^{-1} = hg_2^{-1}$. From this, we obtain by taking inverses that $g = (hg_2^{-1})^{-1} = g_2h^{-1}$, so that

$$g_1H = (g_2h^{-1})H = g_2(h^{-1}H) = g_2H;$$

proving that η is injective.

3-33. Let left cosets are

$$\begin{aligned} &\{1, d\} \\ &\{90, h\} \\ &\{180, a\} \\ &\{270, v\}. \end{aligned}$$

The right cosets are

$$\begin{aligned} &\{1, d\} \\ &\{90, v\} \\ &\{180, a\} \\ &\{270, h\}. \end{aligned}$$

I get 4 of each.

3-39. Let $o(g)$ denote the order of g . For $o(g)$ to equal n means that $g^n = e$, and that $g^k \neq e$ for every $0 < k < n$. If this is so, then

$$(g^{-1})^n = e(g^{-1})^n = g^n(g^{-1})^n = e$$

(by doing n instances of the cancellation $gg^{-1} = e$). Thus, $o(g^{-1}) \leq o(g)$. Since this holds for every g , it also holds for g^{-1} : $o(g^{-1}) \leq o((g^{-1})^{-1}) = o(g)$. Putting these facts together gives $o(g^{-1}) = o(g)$.

3-40. The group table looks like

\cdot	1	g	g^2	g^3
1	1	g	g^2	g^3
g	g	g^2	g^3	1
g^2	g^2	g^3	1	g
g^3	g^3	1	g	g^2

This is not the same as the multiplication table for the 4-group, since in the 4-group, every element except the identity has order 2. It is abelian—the table is symmetric.

3-41. Essentially this is obvious: $g^i g^j = g^{i+j} = g^j g^i$.

If we wanted to be really careful, we would start out by defining powers of g inductively: $g^0 = e$, and $g^{k+1} = g^k g$. This means that our definition of powers results in having them associated so that, for instance, $g^4 = ((gg)g)g$.

We would then do a double induction.

First, we would show that for every k , $g^1 g^k = g^k g^1$. This is obvious for $k = 0$, since $g^1 g^0 = g^1 e = g^1 = e g^1 = g^0 g^1$. Now suppose that $g^1 g^k = g^k g^1$. Then

$$g^1 g^{k+1} = g^1 (g^k g) = (g^1 g^k) g = (g^k g^1) g = (g^k g) g = g^{k+1} g,$$

completing the induction.

Now we prove that for every n and every k , $g^n g^k = g^k g^n$. We already know this holds for $n = 0$ and to $n = 1$. Suppose it holds for n . Then

$$\begin{aligned} g^{n+1} g^k &= (g^n g) g^k = (g g^n) g^k = g(g^n g^k) = g(g^k g^n) = (g g^k) g^n \\ &= (g^k g) g^n = g^k (g g^n) = g^k (g^n g) = g^k g^{n+1}. \end{aligned}$$

This completes the second induction, and with it, the proof.

- 3-42.** It's clear what you want to do. If G and H are finite cyclic groups of order e generated by g and h , resp., then you want to map G to H by sending g^k to h^k . This mapping is clearly 1-to-1 and onto. To see that it's a homomorphism, you need to say something like

$$\phi(g^n g^m) = \phi(g^{(m+n) \bmod e}) = h^{(m+n) \bmod e} = h^m h^n = \phi(g^n) \phi(g^m).$$

Carefully proving the business with the mods is probably an annoying induction rather like the one in the previous problem, and I'm not going to do it.

ADDITIONAL PROBLEM

1. Cayley's Theorem shows that every group G is isomorphic to a subgroup of the group of permutations of the elements of G . There are 6 elements of D_3 ; so Cayley really has us writing D_3 as a subgroup of the permutations of $\{e, \rho, \rho^2, \phi, \phi\rho, \phi\rho^2\}$, a group isomorphic to S_6 . This shows a problem with Cayley: understanding a group isomorphic to S_3 by saying it's isomorphic to a subgroup of S_6 feels like it's moving in the wrong direction.