

Homework One Solutions

- 1.1.16 Let x be an element of G . Prove that $x^2 = 1_G$ if and only if $|x|$ is either 1 or 2.

Proof. (*sufficiency*) Suppose that $x^2 = 1_G$. If $|x| \neq 1$ then $x = x^1 \neq 1_G$. By assumption $x^2 = 1_G$, so 2 is the smallest positive integer n such that $x^n = 1_G$, whence by definition of order, $|x| = 2$.

(*necessity*) Suppose first that $|x| = 1$. Then $x = x^1 = 1_G$, so $x^2 = 1_G \cdot 1_G = 1_G$. If $|x|$ instead is 2, then $x^2 = 1_G$ by definition of order. Thus in either case, $x^2 = 1_G$. \square

- 1.1.17 Let x be an element of G . Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

Proof. Let $|x| = n$. Then $x^n = 1_G$ by definition. Of course $x^n = x \cdot x^{n-1}$, so we have $x \cdot x^{n-1} = 1_G$. Multiplying both sides on the left by x^{-1} we obtain $x^{n-1} = x^{-1}$. \square

- 1.1.31 Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G | g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G \setminus t(G)$ has order 2.]

Proof. Let $t(G) = \{g \in G | g \neq g^{-1}\}$. We note that if $g \neq g^{-1}$ then $g^{-1} \neq (g^{-1})^{-1} = g$, so if $g \in t(G)$, then $g^{-1} \in t(G)$ as well. This implies that the number of elements in $t(G)$ must be even. (If $t(G)$ has an odd number of elements, pair off the inverses, and there is one additional $x \in t(G)$ whose inverse must be in $t(G)$, and hence whose inverse (the others are all paired off) must be x itself, implying $x \notin t(G)$.) Let's say that $\#(t(G)) = 2k$ for some k . Of course $1_G = 1_G^{-1}$, so $1_G \notin t(G)$. At this point we can express G as a disjoint union $G = \{1_G\} \cup t(G) \cup$ the rest of G , and thus $|G| = 1 + 2k + \#(\text{the rest of } G)$. Since $|G|$ is even, there must be at least one element in the rest of G , that is, an element of G neither in $t(G)$ nor equal to 1_G . Such an element must, by definition of $t(G)$, equal its own inverse, and being distinct from 1_G , must have order 2. Thus there must be an element of order 2 in G . \square

- 1.1.32 If x is an element of finite order n in G , prove that the elements $1, x, x^2, \dots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Proof. Suppose by way of contradiction that $x^i = x^k$ for $1 \leq i < k \leq n-1$ (i.e. that the elements $1, x, \dots, x^{n-1}$ are not all distinct). Let $k = i + j$, and observe that by necessity $0 < j < n$. Then

$$\begin{aligned} x^i &= x^k \\ &= x^{i+j} \\ &= x^i x^j. \end{aligned}$$

Multiplying on the left by $(x^i)^{-1}$ we obtain $1_G = x^j$, where, recall $j < n$. Thus n is not the least positive integer power of x to equal 1_G , contradicting the fact that $|x| = n$. We conclude then that the elements $1, x, x^2, \dots, x^{n-1}$ are indeed all distinct. Thus G as a set is the disjoint union of two sets, $G = \{1, x, x^2, \dots, x^{n-1}\} \cup H$ where $H = \{g \in G | g \text{ is not a power of } x\}$. Thus $|G| = \#(\{1, x, x^2, \dots, x^{n-1}\}) + \#(H)$, so $|G| \geq n = |x|$. \square

- 1.2.2 Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r , then $rx = xr^{-1}$.

The elements of D_{2n} which are not powers of r are precisely $\{s, sr, sr^2, \dots, sr^{n-1}\}$. Let $x = sr^j$ be any such element, and consider $rx = rsr^j$. By the relation $rs = sr^{n-1}$ we have

$$\begin{aligned} rx &= rsr^j \\ &= sr^{n-1}r^j \\ &= sr^j r^{n-1} \\ &= sr^j r^{-1} \\ &= xr^{-1} \end{aligned}$$

□

- 1.2.3 Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr , both of which have order 2.

Again, the elements of D_{2n} which are not powers of r are $\{s, sr, sr^2, \dots, sr^{n-1}\}$. Taking sr^j to be one of these elements, we see that

$$\begin{aligned} sr^j sr^j &= sr^{j-1} sr^{n-1} r^j \\ &= sr^{j-2} sr^{2(n-1)} r^j \\ &= sr^{j-3} sr^{3(n-1)} r^j \\ &\dots \\ &= s sr^{j(n-1)} r^j \\ &= (ss) r^{jn-j+j} \\ &= r^{jn} = (r^n)^j = 1 \end{aligned}$$

It remains to show that D_{2n} can be generated by s and sr . Note that $r = s \cdot sr$, so $r^j = (s \cdot sr)^j$, and $sr^j = s(s \cdot sr)^j$. Thus any element of D_{2n} may be written as a product of s and sr . □

- 1.2.7 Show that $\langle a, b | a^2 = b^2 = (ab)^n = 1 \rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s .]

Proof. We are identifying a with s and b with sr , so it follows that we identify ab with $s(sr) = r$. Our proof will take two parts.

First we show that the a, b relations $a^2 = b^2 = (ab)^n = 1$ imply the r, s relations $r^n = s^2 = 1$ and $rs = sr^{n-1}$ with a substituted for s and ab substituted for r . Well, $a^2 = 1$ gives $s^2 = 1$ and $(ab)^n = 1$ gives $r^n = 1$ immediately. We need to check that $(ab)a = a(ab)^{n-1}$ follows from $a^2 = b^2 = (ab)^n = 1$. We begin by noting that

$$\begin{aligned}
a &= a \cdot 1 \\
&= a \cdot (ab)^n \\
&= a(ab)^{n-1} \cdot ab.
\end{aligned}$$

Taking $a = a(ab)^{n-1} \cdot ab$ we multiply on the right by ba to obtain:

$$\begin{aligned}
aba &= a(ab)^{n-1} \cdot ab \cdot ba \\
&= a(ab)^{n-1} \cdot a(bb)a \\
&= a(ab)^{n-1} \cdot aa && \text{using } bb = 1 \\
&= a(ab)^{n-1} && \text{using } aa = 1
\end{aligned}$$

which was what we wanted to show.

Now for the second part we need to show that the a, b relations $a^2 = b^2 = (ab)^n = 1$ follow from the r, s relations ($r^n = s^2 = 1, rs = sr^{n-1}$) when we substitute s for a and sr for b . Clearly $s^2 = 1$ implies $a^2 = 1$. Similarly $r^n = 1$ implies $(ab)^n = 1$. In the problem above, we showed that sr had order 2, so $(sr)^2 = 1$ implies $b^2 = 1$ as well, and we are done. \square