Mathematics 1214: Introduction to Group Theory

Solutions to homework exercise sheet 8

1. Let G be a group and let $a, b \in G$.

   (a) Prove that if $a, b \in G$, then $a = b \iff ab^{-1} = e$.

   (b) Prove that G is an abelian group if and only if $aba^{-1}b^{-1} = e$ for all $a, b \in G$.

   Solution (a) We have $a = b \implies ab^{-1} = bb^{-1} \implies ab^{-1} = e$. and $ab^{-1} = e \implies ab^{-1}b = eb \implies ae = b \implies ab$.

   (b) G is abelian $\iff ab = ba$ for all $a, b \in G \iff ab(ba)^{-1} = e$ for all $a, b \in G$, by (a), $\iff aba^{-1}b^{-1} = e$ for all $a, b \in G$, since $(ba)^{-1} = a^{-1}b^{-1}$ by Theorem 27.

2. [Optional question]
   Let G be a group and let $a \in G$. Prove that for any integers $n, m \in \mathbb{Z}$, we have $a^n a^m = a^{n+m}$. [Suggestion: fix $m \in \mathbb{Z}$ and show that this works for $n = 0$ and $n = 1$, then prove it by induction on n for $n \geq 1$. Finally, think about what happens when $n < 0$.]

   Solution If $n = 0$ then $a^n = e$ so $a^n a^m = a^m$ and $a^{n+m} = a^m$. So this works.

   If $n = 1$ then

$$a^n a^m = aa^m = \left\{ \begin{array}{ll} a(\underbrace{a \dots a}_{m\,\text{times}}) = a^{m+1} & \text{if } m > 0 \\ ae = a^1 & \text{if } m = 0 \\ aa^{-1} = e = a^0 & \text{if } m = -1 \\ a(\underbrace{a^{-1} \dots a^{-1}}_{-m\,\text{times}}) = aa^{-1}(\underbrace{a^{-1} \dots a^{-1}}_{-m-1=-(m+1)\,\text{times}}) = a^{m+1} & \text{if } m < -1 \end{array} \right\} = a^{m+1}$$

   If $n > 0$ and we know that $a^{n-1}a^m = a^{n-1+m}$, then since $a^n = a^1 a^{n-1}$ (by the last paragraph applied with 1 in place of n and $n-1$ in place of m), we have

$$a^n a^m = a^1 a^{n-1} a^m = a^1 a^{n-1+m} \stackrel{*}{=} a^{1+n-1+m} = a^{n+m}$$

   [we have used the result of the last paragraph again at $*$].

   So we have shown that

$$n, m \in \mathbb{Z} \text{ with } n \geq 0 \implies a^n a^m = a^{n+m}. \qquad (\bigstar)$$

   If $n < 0$, let $k = -n$. Since $k > 0$, $(\bigstar)$ gives $a^k a^{-k} = a^0 = e$, so $a^{-k} = (a^k)^{-1}$ by Theorem 27. Now $a^k a^{m-k} = a^m$ by $(\bigstar)$, so multiplying both sides on the left by $a^{-k} = (a^k)^{-1}$ gives $a^{m-k} = a^{-k}a^m$, so $a^{m+n} = a^n a^m$, as desired.

3. Let G be a group and let $a \in G$. Prove that for any integers $n, m \in \mathbb{Z}$, we have $(a^n)^m = a^{nm}$. [Suggestion: fix $n \in \mathbb{Z}$ and show that this works for $m = 0$, and then prove it by induction on m for $m > 0$. Then consider what happens when $m < 0$.]

Solution Fix $n \in \mathbb{Z}$. If $m = 0$ then $(a^n)^m = (a^n)^0 = e$ (since anything to the power of 0 is the identity element, by definition) and $a^{nm} = a^0 = e$. So this case is fine.

Suppose that $m > 0$, and that $(a^n)^{m-1} = a^{n(m-1)}$. Then $(a^n)^m = (a^n)^{m-1}a^m = a^{n(m-1)}a^m = a^{n(m-1)+m} = a^{nm}$. Hence, by induction, $(a^n)^m = a^{nm}$ for all $m \geq 0$.

Now suppose that $m < 0$, and let $k = -m$. Then for any $x \in G$ and $t \in \mathbb{Z}$ we have $x^t x^{-t} = x^0 = e$, so $x^{-t} = (x^t)^{-1}$ by Theorem 27. Applying this to $x = a^n$, $t = k$ and then $x = a$, $t = nk$ and using $(a^n)^k = a^{nk}$ (which we've proven above, since $k > 0$) gives

$$(a^n)^m = (a^n)^{-k} = ((a^n)^k)^{-1} = (a^{nk})^{-1} = a^{-nk} = a^{nm}.$$

4. Disprove the following statements.

   (a) If G is a group and $a, b \in G$ and $n \in \mathbb{Z}$, then $(ab)^n = a^n b^n$.

   (b) If G is a group and $a, b \in G$ and $n \in \mathbb{Z}$, then $(ab)^n = b^n a^n$.

Solution Let $G = S_3$, let $n = 2$ and let $a = (1\ 2)$ and $b = (1\ 2\ 3)$. We have $ab = (1\ 2)(1\ 2\ 3) = (2\ 3)$, so $(ab)^2 = (2\ 3)(2\ 3) = (1)$ and $a^2b^2 = (1\ 2)^2(1\ 2\ 3)^2 = (1)(1\ 3\ 2) = (1\ 3\ 2)$. So $(ab)^2 \neq a^2b^2$, so (a) is false. Similarly, $b^2a^2 = (1\ 3\ 2) \neq (ab)^2$, so (b) is false.

5. Let G be a group and let $a \in G$.

   (a) Show that $\langle a \rangle = \langle a^{-1} \rangle$.

   (b) Deduce from (a) that $o(a) = o(a^{-1})$.

Solution (a) We have $\langle a^{-1} \rangle = \{(a^{-1})^k \colon k \in \mathbb{Z}\} = \{a^{-k} \colon k \in \mathbb{Z}\} = \{a^\ell \colon \ell \in \mathbb{Z}\} = \langle a \rangle$.

(b) By Corollary 32, $o(a) = |\langle a \rangle|$ and $o(a^{-1}) = |\langle a^{-1} \rangle|$, so this is immediate from (a).

6. For each element a in the group $\mathbb{Z}_{10}$, compute $o(a)$ and the cyclic subgroup $\langle a \rangle$.

Solution Note that by exercise 5, the answers for a and a^{-1} are the same. So this nearly halves the amount of calculation we have to do.

a	$o(a)$	$\langle a \rangle$
$[0]$	1	$\{[0]\}$
$[1]$	10	$\mathbb{Z}_{[10]}$
$[2]$	5	$\{[0],[2],[4],[6],[8]\}$
$[3]$	10	$\mathbb{Z}_{[10]}$
$[4]$	5	$\{[0],[4],[8],[12],[16]\} = \{[0],[4],[8],[2],[6]\} = \langle [2] \rangle$
$[5]$	2	$\{[0],[5]\}$
$[6]$	5	$\langle [4] \rangle$ (since $[6] = [4]^{-1}$)
$[7]$	10	$\langle [3] \rangle = \mathbb{Z}_{[10]}$ (since $[7] = [3]^{-1}$)
$[8]$	5	$\langle [2] \rangle$ (since $[8] = [2]^{-1}$)
$[9]$	10	$\langle [1] \rangle = \mathbb{Z}_{[10]}$ (since $[9] = [1]^{-1}$)

7. Let $\mathbb{Q} = \{\frac{n}{m} \colon n, m \in \mathbb{Z},\ m \neq 0\}$ denote the set of rational numbers. It is not hard to show that $(\mathbb{Q}, +)$ is an abelian group. Prove that $(\mathbb{Q}, +)$ is not a cyclic group.

Solution If $\mathbb{Q}$ is cyclic, then $\mathbb{Q} = \langle x \rangle$ for some $x \in \mathbb{Q}$. So $x = \frac{n}{m}$ for some $n, m \in \mathbb{Z}$ with $m \neq 0$, so $\mathbb{Q} = \langle \frac{n}{m} \rangle = \{k\frac{n}{m} : k \in \mathbb{Z}\}$. So the rational number $\frac{n}{2m}$ is in $\mathbb{Q} = \{k\frac{n}{m} : k \in \mathbb{Z}\}$, so there is an integer $k \in \mathbb{Z}$ with $k\frac{n}{m} = \frac{n}{2m}$, so $k = \frac{1}{2}$ and $k \in \mathbb{Z}$, which is a contradiction. So $\mathbb{Q}$ cannot be cyclic.

8. Let $n, m \in \mathbb{Z}$. [As usual, $\mathbb{Z}$ denotes the group $(\mathbb{Z}, +)$.]

   (a) Compute the cyclic subgroups $\langle n \rangle$ and $\langle m \rangle$, and show that

   $$\langle n \rangle \subseteq \langle m \rangle \iff m \mid n.$$

   (b) Find a sequence of $H_1, H_2, H_3, \ldots$ of cyclic subgroups of $\mathbb{Z}$ such that

   $$H_1 \supsetneq H_2 \supsetneq H_3 \supsetneq \ldots.$$

Solution (a) If $m|n$ then $n = km$ for some $k \in \mathbb{Z}$, so

$$\langle n \rangle = \langle km \rangle = \{\ell km : \ell \in \mathbb{Z}\} \subseteq \{tm : t \in \mathbb{Z}\} = \langle m \rangle.$$

So $m|n \implies \langle n \rangle \subseteq \langle m \rangle$.

Conversely, if $\langle n \rangle \subseteq \langle m \rangle$, then since $n \in \langle n \rangle$, we have $n \in \langle m \rangle = \{tm : \ \in \mathbb{Z}\}$, so $n = tm$ for some $t \in \mathbb{Z}$, so $m|n$. Hence $\langle n \rangle \subseteq \langle m \rangle \implies m|n$.

(b) We have $2|2^2|2^3|2^4|\ldots$, so if $H_k = \langle 2^k \rangle$ then $H_1 \supseteq H_2 \supseteq H_3 \supseteq \ldots$ by (a). If $H_k = H_{k+1}$ then $H_k \subseteq H_{k+1}$, so $2^{k+1}|2^k$ by (a), which is false (since $2^{k+1} > 2^k > 0$). This contradiction shows that $H_k \neq H_{k+1}$ for $k \geq 1$. Hence $H_1 \supsetneq H_2 \supsetneq \ldots$.