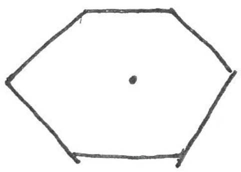
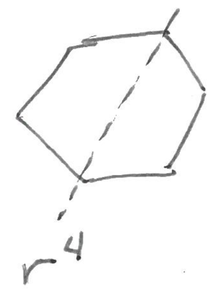


If r is a 60° CCW rotation and v is a vertical reflection describe:

$v \circ r$ = reflection in line:



What is the inverse of r^2? $= r^4$

v? $= v$

$v \circ r$? $= v \circ r$

What is the order of r^4? r^4, $(r^4)^2 = r^8 = r^2$

$(r^4)^3 = r^{12} = r^{2 \cdot 6} = e$

What elements are in $\langle r^4 \rangle$? $= \{r^4, r^2, e\}$

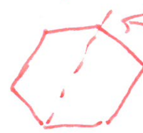
What are all of the cyclic subgroups of D_6?

each of the 6 reflections generates an order 2 cyclic subgroup consisting of e and itself

$\langle e \rangle = \{e\}$, $\langle r \rangle = \langle r^5 \rangle$, $\langle r^2 \rangle = \langle r^4 \rangle = \{r^2, r^4, e\}$, $\langle r^3 \rangle = \{r^3, e\}$

Give an example to show D_6 is not abelian

$v \circ r = r^5 \circ v$, but $v \circ r \neq r \circ v$ reflect in this.



reflect in this

More examples

7.3 # 1b. $U_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$

$\langle 1 \rangle = \{1\}$, $\langle 7 \rangle = \{7, 19, 13, 1\} = \langle 13 \rangle$

$\langle 19 \rangle = \{19, 1\}$ $\langle 11 \rangle = \{11, 1\}$ $\langle 17 \rangle = \{17, 19, 23, 1\}$

$= \langle 23 \rangle$

$\langle 29 \rangle = \{29, 1\}$

Note: none of these generate all of U_{30}, so U_{30} is not a cyclic group.

7.3 # 27. Given $H \leq G$ is a subgroup, and $x \in G$

note: x is constant

$xHx^{-1} = \{xax^{-1} \mid a \in H\}$

this element can change

prove inverses

Let $xax^{-1} \in xHx^{-1}$

then $a \in H$ and $a^{-1} \in H$.

and

$(xax^{-1})(xa^{-1}x^{-1}) =$

$xa(x^{-1}x)a^{-1}x^{-1} =$

$x(aa^{-1})x^{-1}$

$= xx^{-1} = e$

Similarly, $(xa^{-1}x^{-1})(xax^{-1}) = e$

so the inverse of xax^{-1} is $xa^{-1}x^{-1} \in xHx^{-1}$

prove closure

Let $xax^{-1}, xbx^{-1} \in xHx^{-1}$

then $(xax^{-1})(xbx^{-1}) =$

$xa(x^{-1}x)bx^{-1} = xabx^{-1}$

$a, b \in H$, so $ab \in H$

and $xabx^{-1} \in xHx^{-1}$

so xHx^{-1} is a subgroup of G.

7.3 #28a. G is an abelian group, $n > 0$ is an integer

Prove: $H = \{a \in G \mid a^n = e\}$ is a subgroup.

note: $e^n = e$ for every n, so $e \in H$ ∴ H is not empty.

Inverses

Let $a \in H$.

then $a^n = e$

$(a^{-1})^n (a^n) = (a^{-1}a)^n$ (abelian)

$= e^n = e$

so $(a^{-1})^n a^n = e$

$(a^{-1})^n \cdot e = e$

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

so $a^{-1} \in H$.

closure

Let $a, b \in H$

then $a^n = e$ and $b^n = e$

$(ab)^n = a^n b^n$ (abelian)

$= e \cdot e = e$

so, $ab \in H$.

7.4 #6. Let $h: \mathbb{Z}_8 \to \mathbb{Z}_8$ $h(x) = 2x$

Let $a, b \in \mathbb{Z}_8$. Then $h(a+b) = 2(a+b) = 2a + 2b$

$= h(a) + h(b)$

so h is a homomorphism

x	$h(x)$
0	0
1	2
2	4
3	6
4	0

x	$h(x)$
5	2
6	4
7	6

3 is not in the image, so h is not onto

$h(1) = h(5)$ so h is not 1-to-1

Thm 7.19 b.

G is a cyclic group

so G is generated by $a \in G$

$\langle a \rangle = G$

G has order n

$\{ e = \underset{\substack{\shortparallel \\ a^n}}{a^0}, a^1, a^2, a^3, a^4, \ldots a^{n-1} \}$

---

so $G \cong \mathbb{Z}_n$

Let $f: G \to \mathbb{Z}_n$ such that

$f(a^k) = [k]_n$

---

one-to-one:

if $a^i, a^j \in G$

$f(a^i) = f(a^j)$

$[i]_n = [j]_n$

$j = i + mn$

$a^j = a^{i+mn} = a^i \underset{\substack{\shortparallel \\ e}}{a^{mn}} = a^i$

onto:

Let $[i] \in \mathbb{Z}_n$

then $a^i \in G$

$f(a^i) = [i]$

so f is onto.

Let $a^i, a^j \in G$

$f(a^i \cdot a^j) = f(a^{i+j}) = [i+j] = [i] + [j]$

$= f(a^i) + f(a^j)$

so $f(\underset{G}{a^i} \cdot \underset{G}{a^j}) = \underbrace{f(a^i)}_{\mathbb{Z}_n} + \underbrace{f(a^j)}_{\mathbb{Z}_n}$ so f is a homomorphism.

14. prove $\mathbb{Z}_6, + \cong \underbrace{\mathbb{Z}_7^*, \cdot = U_7}$ $= \{1, 2, 3, 4, 5, 6\}$

$$\mathbb{Z}_6 = \langle 1 \rangle = \{1, 2\cdot 1, 3\cdot 1, 4\cdot 1, 5\cdot 1, 6\cdot 1 = 0 = e\}$$

Cyclic subgroups

$\langle 1 \rangle = \{1\}$ $\quad \langle 2 \rangle = \{2, 4, 1\}$ 2^2 (order 3)

$$\langle 3 \rangle = \{3, \underset{3^2}{2}, \underset{3^3}{6}, \underset{3^4}{4}, \underset{3^5}{5}, \underset{3^6}{1}\}$$

3 generates $\mathbb{Z}_7^*$

$f: U_7 \to \mathbb{Z}_6 \qquad f(3^i) = [i]_6$

$g: \mathbb{Z}_6 \to U_7 \qquad g([i]_6) = 3^i \in \mathbb{Z}_7$

prove it's an isomorphism like Thm 19 b.

$g:$
$0 \to 1 = 3^0 = 3^6$
$1 \to 3^1 = 3$
$2 \to 3^2 = 2$
$3 \to 3^3 = 6$
$4 \to 3^4 = 4$
$5 \to 3^5 = 5$

every element in $U_7 = \mathbb{Z}_7^*$ is mapped to once and only once, so it is 1-to-1 and onto

Let $i, j \in \mathbb{Z}_6$

then $g(i+j) = 3^{i+j} = 3^i \cdot 3^j = g(i)\,g(j)$ so g is a homomorphism.

7.4 #13 show $U_5 \cong U_{10}$

$U_5 = \{1, 2, 3, 4\}$ $\quad$ $U_{10} = \{1, 3, 7, 9\}$

$\langle 2 \rangle = \{\underset{2^1}{2}, \underset{2^2}{4}, \underset{2^3}{3}, \underset{2^4}{1}\}$ $\quad$ $\langle 3 \rangle = \{\underset{3^1}{3}, \underset{3^2}{9}, \underset{3^3}{7}, \underset{3^4}{1}\}$

using 7.19 b:

By thm 7.19, $U_5 \cong \mathbb{Z}_4$ and $U_{10} \cong \mathbb{Z}_4$

so $U_5 \cong U_{10}$

Without using thm 19:

Let $f : U_5 \to U_{10}$ such that $f([2^i]_5) = [3^i]_{10}$

(check f is a function) if $2^i = 2^j$ then $2^{j-i} = 1$ so $j-i = 4 \cdot k$
$j = i + 4k$

so $f(2^j) = [3^j]_{10} = [3]_{10}^{i+4k} = [3]_{10}^i \cdot \underbrace{[3]_{10}^{4k}}_{=1} = [3]_{10}^i$

check f is one-to-one and onto

$$f: \left.\begin{array}{l} 2 \to 3 \\ 4 \to 9 \\ 3 \to 7 \\ 1 \to 1 \end{array}\right\}$$ each element of U_{10} appears once and only once, so f is one-to-one and onto.

Let $2^i, 2^j \in U_5$.

Then $f(2^i \cdot 2^j) = f(2^{i+j}) = 3^{i+j} = 3^i \cdot 3^j = f(2^i) f(2^j)$

So f is a homomorphism.

Thus f is an isomorphism.

7.4 #13 alternate proof of 1-1 and onto:

one-to-one

Let $2^i, 2^j \in U_5$

such that

$f(2^i) = f(2^j)$

then $3^i = 3^j$

$\Rightarrow 3^{j-i} = 1$

$j - i = 4k \quad (k \in \mathbb{Z})$

$j = i + 4k$

$2^j = 2^{i+4k} = 2^i \cdot 2^{4k} = 2^i \cdot 1 = 2^i$

so f is one-to-one

onto

Let $3^i \in U_{10}$

then $2^i \in U_{10}$

and $f(2^i) = 3^i$

so f is onto.

7.4 #8 Let $g: \mathbb{R} \to \mathbb{R}^*$ such that $g(x) = 2^x$

1-to-1

Let $a, b \in \mathbb{R}$ such that

$g(a) = g(b)$

$2^a = 2^b$

$\log_2(2^a) = \log_2(2^b)$

$a = b$

so g is one-to-one

homomorphism

Let $a, b \in \mathbb{R}$

note $\mathbb{R}, +$ and $\mathbb{R}^*, \cdot$

$g(a+b) = 2^{(a+b)} = 2^a \cdot 2^b$

$= g(a) \cdot g(b)$

so g is a homomorphism.

$-1 \in \mathbb{R}^*$, but $2^x > 0$ for all $x \in \mathbb{R}$, so g is not onto.

Note: $g: \mathbb{R} \to \mathbb{R}^{**}$ such that $g(x) = 2^x$ is an isomorphism.

if $a \in \mathbb{R}^{**}$ then $\log_2(a) \in \mathbb{R}$

and $g(\log_2(a)) = 2^{\log_2(a)} = a$.