Homomorphism and subgroups

Tuesday, June 29, 2021 3:29 PM

Whenever we learn about a new structure in mathematics, we should study the functions between these objects that preserve their properties. These functions are often called homomorphism. (In a very vague sense homomorphisms give us a global understanding of the objects.) Another point of view is from inside: we often study subsets that share the same property. For instance in linear algebra, the objects of interest are vector spaces, the homomorphisms are linear maps, and subsets that share the same properties are subspaces. We do the same for groups.

Def.. Suppose $(G, \cdot)$ and $(H, *)$ are two groups. Then a function $f: G \to H$ is called a group homomorphism if for every $g_1, g_2 \in G$, $f(g_1 \cdot g_2) = f(g_1) * f(g_2)$.

• Suppose $(G, \cdot)$ is a group. Then a subset K of G is called a subgroup of G if K is a group with respect to the operation $\cdot$.

Next we see a few examples.

Examples of group homomorphisms

Tuesday, June 29, 2021 3:29 PM

Ex. Suppose n is an integer and $n \geq 2$. Then

$$c_n: \mathbb{Z} \to \mathbb{Z}_n, \quad c_n(a) := [a]_n$$

is a group homomorphism.

Solution. For every $a, b \in \mathbb{Z}$,

$$c_n(a+b) = [a+b]_n = [a]_n + [b]_n = c_n(a) + c_n(b). \quad \blacksquare$$

Ex. $f: \mathbb{Z} \to \mathbb{Z}$, $f(x) = -x$ is a group homomorphism.

Solution. For every $x, y \in \mathbb{Z}$,

$$f(x+y) = -(x+y) = (-x) + (-y) = f(x) + f(y). \quad \blacksquare$$

Ex. Let $\mathbb{R}^{>0}$ be the set of positive real numbers. Notice that $\mathbb{R}^{>0}$ is a group under multiplication. Then

$\ln: \mathbb{R}^{>0} \to \mathbb{R}$ is a group homomorphism.

Solution. For every $x, y \in \mathbb{R}^{>0}$,

$$\ln(x \cdot y) = \ln(x) + \ln(y). \quad \blacksquare$$

Ex. Let $N: \mathbb{C} \setminus \{0\} \to \mathbb{R}^{>0}$, $N(z) = |z|$. Then N is a group homomorphism.

Solution. For every $z \in \mathbb{C} \setminus \{0\}$, $|z| \in \mathbb{R}^{>0}$ and $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$. $\blacksquare$

Examples of group homomorphisms

Tuesday, June 29, 2021 3:29 PM

Ex. Let $GL_n(\mathbb{R})$ be the set of invertible $n\times n$ real matrices.

From linear algebra we know that matrix multiplication is associative, product of two invertible $n\times n$ matrices is invertible, for every a in $GL_n(\mathbb{R})$, $a\cdot I_n = I_n\cdot a = a$ where I_n is the identity matrix. So $(GL_n(\mathbb{R}),\cdot)$ is a group. Let $\theta: GL_n(\mathbb{R}) \to GL_n(\mathbb{R})$, $\theta(x) = (x^t)^{-1}$ where x^t is the transpose of x. Then θ is a group homomorphism.

Solution. $\theta(x\cdot y) = ((x\cdot y)^t)^{-1} = (y^t\cdot x^t)^{-1} = (x^t)^{-1}\cdot(y^t)^{-1}$

$$= \theta(x)\cdot\theta(y). \qquad \blacksquare$$

Ex. Suppose $(G,\cdot)$ is a group. Then $f: G \to G$, $f(g) = g^{-1}$ is a group homomorphism if and only if G is abelian.

Solution. ($\Rightarrow$) For every $g,h\in G$, $f(g\cdot h) = f(g)\cdot f(h)$. Then

$(g\cdot h)^{-1} = g^{-1}\cdot h^{-1} \Rightarrow h^{-1}\cdot g^{-1} = g^{-1}\cdot h^{-1}$. (I)

For $x,y\in G$, let $g = x^{-1}$ and $h = y^{-1}$ in (I). Then we obtain $(y^{-1})^{-1}\cdot(x^{-1})^{-1} = (x^{-1})^{-1}\cdot(y^{-1})^{-1}$. Since $(x^{-1})^{-1} = x$ and $(y^{-1})^{-1} = y$, we conclude $y\cdot x = x\cdot y$. Therefore G is abelian.

($\Leftarrow$) $f(g\cdot h) = (g\cdot h)^{-1} = h^{-1}\cdot g^{-1} = f(h)\cdot f(g) \overset{\text{abelian}}{=} f(g)\cdot f(h)$. $\blacksquare$

Examples of group homomorphisms

Tuesday, June 29, 2021 3:29 PM

<u>Ex.</u> Suppose $(G,\cdot)$ is a group and $g\in G$. Let

$$c_g : G \to G, \quad c_g(x) := g\cdot x\cdot g^{-1}.$$

Then c_g is a group homomorphism.

<u>Solution.</u> For $x,y\in G$, we have to show that

$$c_g(x\cdot y) \overset{?}{=} c_g(x)\cdot c_g(y).$$

We have $\quad c_g(x\cdot y) = g\cdot x\cdot y\cdot g^{-1}$ (I) and

$$\begin{aligned} c_g(x)\cdot c_g(y) &= (g\cdot x\cdot g^{-1})\cdot(g\cdot y\cdot g^{-1}) \\ &= g\cdot x\cdot (g^{-1}\cdot g)\cdot y\cdot g^{-1} \\ &= g\cdot x\cdot e_G\cdot y\cdot g^{-1} \\ &= g\cdot x\cdot y\cdot g^{-1} \qquad \text{(II)} \end{aligned}$$

By (I) and (II), we obtain that $c_g(x\cdot y) = c_g(x)\cdot c_g(y)$. ■

<u>Ex.</u> Suppose $(G,\cdot)$ is a group and $g\in G$. Then

$$f:\mathbb{Z}\to G,\quad f(n):=g^n \text{ is a group homomorphism.}$$

<u>Solution.</u> For every $m,n\in\mathbb{Z}$,

$$f(m+n) = g^{m+n} = g^m\cdot g^n = f(m)\cdot f(n). \qquad ■$$

Examples of subgroups

Tuesday, June 29, 2021 3:29 PM

Ex. $\mathbb{Z}$ is a subgroup of $(\mathbb{Q},+)$. $\mathbb{Q}$ is a subgroup of $(\mathbb{R},+)$.

$\mathbb{R}$ is a subgroup of $(\mathbb{C},+)$.

Ex. $2\mathbb{Z} := \{2k \mid k\in\mathbb{Z}\}$ is a subgroup of $(\mathbb{Z},+)$.

Pf. . For every $k,l\in\mathbb{Z}$, $2k+2l=2(k+l)\in 2\mathbb{Z}$, and so $+$ defines an operation on $2\mathbb{Z}$

. $+$ is associative.

. $0=(2)(0)\in 2\mathbb{Z}$ and, for every $x\in 2\mathbb{Z}$, $x+0=0+x=x$.

. If $x\in 2\mathbb{Z}$, then $x=2k$ for some $k\in\mathbb{Z}$. Hence $-x=2(-k)\in 2\mathbb{Z}$, and $x+(-x)=(-x)+x=0$. ∎

Ex. $\mathbb{R}\setminus\{0\}$ is not a subgroup of $(\mathbb{R},+)$.

Solution. $1,-1$ are in $\mathbb{R}\setminus\{0\}$, but $1+(-1)=0$ is not in $\mathbb{R}\setminus\{0\}$ ∎

Ex. Suppose $(G,\cdot)$ is a group. Then $\{e_G\}$ is a subgroup of G.

Solution. . $e_G\cdot e_G=e_G$. Hence $\cdot$ defines an operation on $\{e_G\}$.

. $\cdot$ is associative. . $e_G\in\{e_G\}$. $e_G^{-1}=e_G$. ∎

Some parts of these arguments seem to be redundant. The next criterion helps us avoid these redundancies.

Subgroup criterion and more examples

Tuesday, June 29, 2021 3:29 PM

Lemma (Subgroup criterion) Suppose $(G, \cdot)$ is a group. A subset H of G is a subgroup if it is not empty and for every $x, y \in H$, $x \cdot y^{-1} \in H$.

Pf. Since $H \neq \emptyset$, there is $x_0 \in H$. By hypothesis, $x_0 \cdot x_0^{-1} \in H$, which means $e_G \in H$. (I)

. For every $y \in H$, by hypothesis and (I), $e_G \cdot y^{-1} \in H$, which means $y^{-1} \in H$. (II)

. For every $x, y \in H$, by (II) $y^{-1} \in H$, and so by hypothesis, $x \cdot (y^{-1})^{-1} \in H$. This implies $x \cdot y \in H$ as $(y^{-1})^{-1} = y$. Therefore for every $x, y \in H$, $x \cdot y \in H$. Hence $\cdot$ defines an operation on H.

. $\cdot$ is associative.

. By (I), H has the neutral element of $\cdot$.

. By (II), every element of H has an inverse in H. ∎

Let us make two important remarks about subgroups in form of a lemma. This is a subtle and important lemma that we often use.

Basic property of subgroups and examples

Tuesday, June 29, 2021 3:29 PM

Lemma (Basic property of subgroups) Suppose H is a subgroup of $(G, \cdot)$. Then the neutral element e_G of G is in H, and, for every $x, y \in H$, $x \cdot y^{-1} \in H$ where y^{-1} is the inverse of y in G.

Pf. Since H is a subgroup, it has a neutral element e_H. Hence $e_H \cdot e_H = e_H$ (I). Multiplying both sides of (I) by the inverse e_H^{-1} of e_H in G, we obtain

$\underbrace{e_H \cdot e_H \cdot e_H^{-1}}$ ... more precisely: $e_H \cdot \underbrace{e_H \cdot e_H^{-1}}_{e_G} = \underbrace{e_H \cdot e_H^{-1}}_{e_G}$; and so $e_H = e_G$ (II). Thus $e_G \in H$. Because H is a subgroup, every element of H has an inverse in H. Hence if $y \in H$, then there is $y' \in H$ such that $y \cdot y' = e_H$. By (II), $y \cdot y' = e_G$ (III). Multiplying both sides of (III) by y^{-1}, we obtain $\underbrace{y^{-1} \cdot y}_{e_G} \cdot y' = y^{-1}$, and so $y' = y^{-1}$ is in H. Thus, for $x, y \in H$, $x \cdot y^{-1} \in H$. ∎

Ex. For every $n \in \mathbb{Z}$, $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

Solution. Notice that $0 = (n)(0) \in n\mathbb{Z}$, and so it is non-empty. For x, y in $n\mathbb{Z}$, $x = nk$ and $y = nl$ for some $k, l \in \mathbb{Z}$. Then $x - y = nk - nl$,

Centralizer subgroups

Tuesday, June 29, 2021 3:29 PM

which implies that $x-y = n(k-\ell) \in n\mathbb{Z}$. Therefore by the subgroup criterion $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. ∎

Ex. (Centralizer) Suppose $(G,\cdot)$ is a group and $g \in G$. Then $C_G(g) := \{x \in G \mid g\cdot x = x \cdot g\}$ is called the centralizer of g, and it is a subgroup of G.

Pf. . Let e_G be the neutral element of G. Then $e_G \cdot g = g = g \cdot e_G$. Hence $e_G \in C_G(g)$, which implies that $C_G(g)$ is not empty.

. Suppose $x, y \in C_G(g)$. This means $\overset{(\mathrm{I})}{x\cdot g = g\cdot x}$ and $\overset{(\mathrm{II})}{y\cdot g = g\cdot y}$. We want to show that $x\cdot y^{-1} \in C_G(g)$. So we start by wondering what (I) and (II) say about y^{-1}. Multiplying both sides of (II) by y^{-1} from left and right, we obtain

$$y\cdot g = g\cdot y \Rightarrow y^{-1}\cdot(y\cdot g)\cdot y^{-1} = y^{-1}\cdot(g\cdot y)\cdot y^{-1}$$

$$\Rightarrow \underbrace{y^{-1}\cdot y}_{e_G}\cdot g\cdot y^{-1} = y^{-1}\cdot g\cdot \underbrace{y\cdot y^{-1}}_{e_G}$$

$$\Rightarrow \quad g\cdot y^{-1} = y^{-1}\cdot g \qquad (\mathrm{III})$$

$(x\cdot y^{-1})\cdot g = x\cdot(y^{-1}\cdot g) \overset{(\mathrm{III})}{=} x\cdot g\cdot y^{-1} \overset{(\mathrm{I})}{=} g\cdot x\cdot y^{-1}$. This

Center

Tuesday, June 29, 2021 3:29 PM

means $x \cdot y^{-1} \in C_G(g)$. Hence by the subgroup criterion $C_G(g)$ is a subgroup of G. ∎

<u>Ex.</u> (Center) Suppose $(G, \cdot)$ is a group. Then $Z(G) := \{x \in G \mid \forall g \in G,\ g \cdot x = x \cdot g\}$ is called the center of G, and it is a subgroup of G.

<u>Pf.</u> Suppose e_G is the neutral element of G. Then for every $g \in G$, $g \cdot e_G = e_G \cdot g = g$. Hence $e_G \in Z(G)$. So $Z(G)$ is not empty.

- Suppose $x, y \in Z(G)$; we want to show that $x \cdot y^{-1} \in Z(G)$.

Since $x, y \in Z(G)$, for every $g \in G$, $x \cdot g = g \cdot x \ \text{(I)}$ and $y \cdot g = g \cdot y \ \text{(II)}$.

By (I) and (II), $x, y \in C_G(g)$. Because $C_G(g)$ is a subgroup, we conclude that $x \cdot y^{-1} \in C_G(g)$. Therefore $(x \cdot y^{-1}) \cdot g = g \cdot (x \cdot y^{-1}) \ \text{(III)}$.

Since (III) holds for every $g \in G$, we deduce that $x \cdot y^{-1} \in Z(G)$. Therefore by the subgroup criterion $Z(G)$ is a subgroup. ∎

Notice that $Z(G) = \bigcap_{g \in G} C_G(g)$, and so the next example

Intersection.

Tuesday, June 29, 2021 3:29 PM

gives us an alternative approach for proving that $Z(G)$ is a subgroup.

<u>Ex.</u> (Intersection of subgroups) Suppose $\{H_i\}_{i\in I}$ is a family of subgroups of $(G,\cdot)$. Then $\bigcap_{i\in I} H_i$ is a subgroup of G.

<u>Pf</u> Let $H := \bigcap_{i\in I} H_i$. Since H_i is a subgroup of G, the neutral element e_G of G is in H_i. Hence $e_G \in \bigcap_{i\in I} H_i$. Thus H is not empty.

Suppose $x,y\in H$. We want to show $x\cdot y^{-1}\in H$. Because $x,y\in \bigcap_{i\in I} H_i$, for every $i\in I$, $x,y\in H_i$. Since H_i is a subgroup of G, $x\cdot y^{-1}\in H_i$. Thus $x\cdot y^{-1}\in \bigcap_{i\in I} H_i$.

Therefore by the subgroup criterion $\bigcap_{i\in I} H_i$ is a subgroup. ∎

Next we explore some of the connections between group homomorphisms and subgroups. Suppose $(G,\cdot)$ and $(H,*)$ are two groups, and $f: G\to H$ is a group homomorphism. Let $\mathrm{Im}(f)$ be the image of f; that

Image and kernel of homomorphisms

Tuesday, June 29, 2021 3:29 PM

is $\mathrm{Im}(f) := \{f(g) \mid g \in G\}$, and similar to linear algebra let the kernel of f be

$$\ker(f) := \{g \in G \mid f(g) = e_H\}$$

where e_H is the neutral element of H.

<u>Theorem.</u> Suppose $(G, \cdot)$ and $(H, *)$ are groups, and $f: G \to H$ is a group homomorphism. Then $\mathrm{Im}(f)$ is a subgroup of H, and $\ker(f)$ is a subgroup of G.

Proof of this theorem is based on the following properties of a group homomorphism.

<u>Proposition</u> (Basic properties of group homomorphisms) Suppose $f: G \to H$ is a group homomorphism. Then

(1) $f(e_G) = e_H$ where e_G is the neutral element of G, and e_H is the neutral element of H, and

(2) For every $g \in G$, $f(g^{-1}) = f(g)^{-1}$ where g^{-1} is the inverse of g in G and $f(g)^{-1}$ is the inverse of $f(g)$ in H.

<u>Pf of proposition.</u> (1) Since e_G is the neutral element of G,

Basic properties of homomorphisms

Tuesday, June 29, 2021 3:29 PM

$e_G \cdot e_G = e_G$. Because f is a group homomorphism, $f(e_G \cdot e_G) = f(e_G)\cdot f(e_G)$. Hence $f(e_G)\cdot f(e_G) = f(e_G)$. Thus $f(e_G)\cdot f(e_G) = f(e_G)\cdot e_H$. Therefore by the cancellation law, $f(e_G) = e_H$.

(2) For every $g \in G$, $g \cdot g^{-1} = e_G$. Applying f to the both sides, we obtain that $f(g\cdot g^{-1}) = f(e_G)$. By the 1st part and the fact that f is a group homomorphism, we deduce that $f(g)\cdot f(g^{-1}) = e_H$. Multiplying both sides by the inverse $f(g)^{-1}$ of $f(g)$ in H, we obtain

$$\underbrace{f(g)^{-1}\cdot f(g)}_{e_H}\cdot f(g^{-1}) = f(g)^{-1}\cdot e_H \text{; and so } f(g^{-1}) = f(g)^{-1}.$$

Now we are ready to prove that $\mathrm{Im}(f)$ and $\ker(f)$ are subgroups.

<u>Pf of Theorem.</u> Notice that $f(e_G) \in \mathrm{Im}(f)$, and so $\mathrm{Im}(f)$ is not empty. Suppose $\bar{x}, \bar{y} \in \mathrm{Im}(f)$. Then $\bar{x} = f(x)$ and $\bar{y} = f(y)$ for some $x, y \in G$. We want to show $\bar{x} * \bar{y}^{-1} \in \mathrm{Im} f$.

Image and kernel

Tuesday, June 29, 2021 3:29 PM

$$\bar{x} * \bar{y}^{-1} = f(x) * f(y)^{-1}$$

$$= f(x) * f(y^{-1}) \quad \text{(properties of homomorphisms)}$$

$$= f(x \cdot y^{-1}) \quad \text{(} f \text{ is a homomorphism)}$$

$$\in \mathrm{Im}(f).$$

Hence by the subgroup criterion $\mathrm{Im}(f)$ is a subgroup of H.

- By the properties of homomorphisms, $f(e_G) = e_H$. Hence $e_G \in \ker(f)$. Suppose $x, y \in \ker f$. We want to show $x \cdot y^{-1} \in \ker(f)$.

$$f(x \cdot y^{-1}) = f(x) * f(y^{-1}) \quad \text{(} f \text{ is a homomorphism)}$$

$$= f(x) * f(y)^{-1} \quad \text{(properties of hom.)}$$

$$= e_H * e_H^{-1} \quad (x, y \in \ker f)$$

$$= e_H \quad (e_H^{-1} = e_H)$$

Therefore by the subgroup criterion $\ker f$ is a subgroup. ■

Ex. Find the kernel and the image of $c_n : \mathbb{Z} \to \mathbb{Z}_n$, $c(a) := [a]_n$.

Solution. Every element of $\mathbb{Z}_n$ is of the form $[a]_n$ for some a in $\mathbb{Z}$. Hence every element of $\mathbb{Z}_n$ is in $\mathrm{Im}(c_n)$. An integer a

Image and kernel

Tuesday, June 29, 2021 3:29 PM

is in the kernel of c_n if and only if $c_n(a) = [0]_n$.

$$c_n(a) = [0]_n \iff [a]_n = [0]_n$$
$$\iff a \overset{n}{\equiv} 0$$
$$\iff a \in n\mathbb{Z}.$$

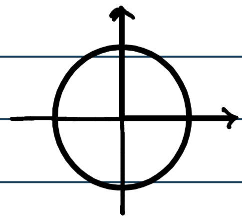
Hence $\ker c_n = n\mathbb{Z}$. ∎

<u>Ex.</u> Let's recall that $N: \mathbb{C}\setminus\{0\} \to \mathbb{R}^{>0}$, $N(z) := |z|$ is a group homomorphism. Find the image and the kernel of N.

<u>Solution.</u> . For every $r \in \mathbb{R}^{>0}$, $N(r) = r$. Hence $\mathrm{Im}(N) = \mathbb{R}^{>0}$.

. $z \in \ker(N) \iff N(z) = 1 \iff |z| = 1$. Therefore

$\ker(N) = \{z \in \mathbb{C} \mid |z| = 1\}$ is the unit circle centered at the origin. ∎



The unit circle centered at the origin is often denoted by S^1.

As a corollary of the above example, we obtain that

. S^1 is a subgroup of $(\mathbb{C}\setminus\{0\}, \cdot)$.

<u>Ex.</u> Let $f: \mathbb{R} \to S^1$, $f(x) := e^{2\pi i x}$. Argue that f is a group homomorphism, and find $\mathrm{Im}(f)$ and $\ker(f)$.

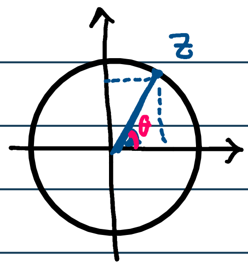
Image and kernel

Tuesday, June 29, 2021 3:29 PM

<u>Solution</u>. For every $x_1, x_2 \in \mathbb{R}$,

$$f(x_1+x_2) = e^{2\pi i (x_1+x_2)}$$
$$= e^{2\pi i x_1 + 2\pi i x_2}$$
$$= e^{2\pi i x_1} \cdot e^{2\pi i x_2}$$
$$= f(x_1) \cdot f(x_2).$$

Hence f is a group homomorphism.



- Every $z \in S^1$ is of the form $\cos\theta + i \sin\theta$, and so by Euler's formula $z = e^{i\theta}$. Therefore $z = f\left(\frac{\theta}{2\pi}\right)$ is in the image of f. Thus $\mathrm{Im}(f) = S^1$.

- $x \in \ker(f) \iff f(x) = 1$

$$\iff e^{2\pi i x} = 1$$
$$\iff 2\pi x \text{ is an integer multiple of } 2\pi.$$
$$\iff x \in \mathbb{Z}.$$

Therefore $\ker(f) = \mathbb{Z}$. ▤

Finally let's find out centers and some centralizer subgroups of S_n and D_{2n}.

Center of symmetric groups

Tuesday, June 29, 2021 3:29 PM

Ex. $Z(S_n)=\{id.\}$ if $n\geq 3$.

Pf. Suppose to the contrary that there $\sigma\in Z(S_n)\setminus\{id.\}$.
Then $\sigma(i)\neq i$ for some $i\in[1..n]$. Suppose $\sigma(i)=j\neq i$.
Since $n\geq 3$, there is $k\in[1..n]\setminus\{i,j\}$. Let τ be the permutation which flips i and k; that means

$\tau(i)=k$, $\tau(k)=i$, and $\tau(r)=r$ if $r\in[1..n]\setminus\{i,k\}$.

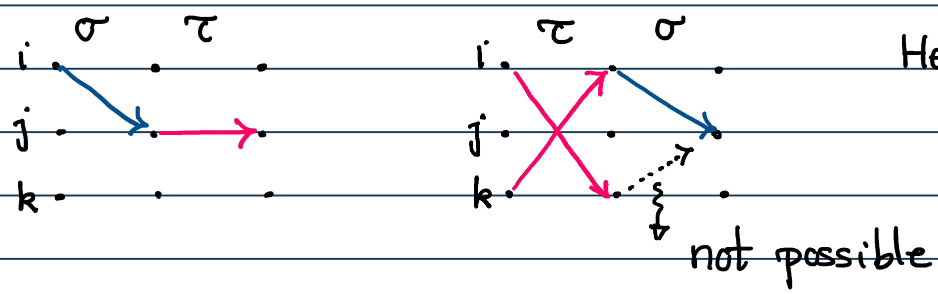
Consider $\tau\circ\sigma(i)$ and $\sigma\circ\tau(i)$. We have

$\tau\circ\sigma(i)=\tau(j)=j$ as $j\notin\{i,k\}$ (I) and

$\sigma\circ\tau(i)=\sigma(k)$. (II)

Since $i\neq k$ and σ is a permutation, $\sigma(i)\neq\sigma(k)$, which means $j\neq\sigma(k)$. (III)

By (I), (II), and (III), $\tau\circ\sigma\neq\sigma\circ\tau$ which contradicts the assumption that σ is in the center of S_n. ∎



Hence $\tau\circ\sigma\neq\sigma\circ\tau$.

More on dihedral groups

Tuesday, June 29, 2021 3:29 PM

Let's recall that $D_{2n} = \{id., \sigma, \ldots, \sigma^{n-1}, \tau, \sigma\circ\tau, \ldots, \sigma^{n-1}\circ\tau\}$

where $\sigma: \mathbb{Z}_n \to \mathbb{Z}_n$, $\sigma(x) = x + [1]_n$.

and $\tau: \mathbb{Z}_n \to \mathbb{Z}_n$, $\tau(x) = -x$.

Notice that $\sigma^i(x) = x + [i]_n$ for every integer i. In particular $\sigma^i = id. \Leftrightarrow [i]_n = [0]_n \Leftrightarrow n \mid i$. (I)

$\tau^2(x) = \tau(-x) = -(-x) = x$; and so $\tau^2 = id.$, and

$\tau\circ\sigma^i\circ\tau^{-1}(x) = \tau(\sigma^i(-x)) = \tau(-x+[i]_n)$

$= x + [-i]_n = \sigma^{-i}(x)$; and so

$\tau\circ\sigma^i\circ\tau^{-1} = \sigma^{-i}$. (II)

<u>Proposition</u> $C_{D_{2n}}(\tau) = \{id., \tau\}$ if n is odd, and

$C_{D_{2n}}(\tau) = \{id., \tau, \sigma^{n/2}, \sigma^{n/2}\circ\tau\}$ if n is even.

<u>Pf</u> Clearly $\tau \in C_{D_{2n}}(\tau)$ as $\tau\circ\tau = \tau\circ\tau$! Suppose σ^i is in $C_{D_{2n}}(\tau)$. Then $\tau\circ\sigma^i = \sigma^i\circ\tau$, which implies that $\tau\circ\sigma^i\circ\tau^{-1} = \sigma^i$. Hence, by (II), $\sigma^{-i} = \sigma^i$. Multiplying both sides by σ^i, we deduce that $\sigma^{2i} = id.$ By (I), we conclude that $n \mid 2i$. If n is odd, then $\gcd(n,2) = 1$.

Center of dihedral groups

Tuesday, June 29, 2021 3:29 PM

By Euclid's lemma, $n \mid 2i$ and $\gcd(n,2)=1$ imply that $n \mid i$, and so $\sigma^i = \mathrm{id}.$ Hence

if n is odd, $\{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\} \cap C_{D_{2n}}(\tau) = \{\mathrm{id}.\}$. (I)

If n is even, $n \mid 2i$ implies that $\frac{n}{2} \mid i$. Conversely if $\frac{n}{2} \mid i$, then $n \mid 2i$. In this case $\tau \circ \sigma^i = \sigma^i \circ \tau$. Thus

if n is even, $\{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\} \cap C_{D_{2n}}(\tau) =$

$$\{\sigma^i \mid \tfrac{n}{2} \mid i \text{ and } 0 \le i < n\} = \{\mathrm{id}., \sigma^{n/2}\}. \quad \text{(II)}$$

. Since $C_{D_{2n}}(\tau)$ is a subgroup and $\tau \in C_{D_{2n}}(\tau)$, we have

$$\sigma^i \circ \tau \in C_{D_{2n}}(\tau) \iff \sigma^i \in C_{D_{2n}}(\tau). \quad \text{(III)}$$

By (I), (II), and (III) we conclude that

$$C_{D_{2n}}(\tau) = \{\mathrm{id}., \tau\} \text{ if } n \text{ is odd, and}$$

$$C_{D_{2n}}(\tau) = \{\mathrm{id}., \sigma^{n/2}, \tau, \sigma^{n/2} \circ \tau\}. \quad \blacksquare$$

Proposition. $Z(D_{2n}) = \{\mathrm{id}.\}$ if $n > 1$ and odd, and

$$Z(D_{2n}) = \{\mathrm{id}., \sigma^{n/2}\} \text{ if } n > 2 \text{ and even}.$$

Pf. Notice that $Z(D_{2n}) \subseteq C_{D_{2n}}(\tau)$ (IV). Suppose n is odd.

By (IV) and the previous proposition, to show $Z(D_{2n}) = \{\mathrm{id}.\}$,

Center of dihedral groups

Tuesday, June 29, 2021 3:29 PM

it is enough to show $\tau \notin Z(D_{2n})$. Suppose to the contrary that $\tau \in Z(D_{2n})$. Then $C_{D_{2n}}(\tau) = D_{2n}$, and so $|C_{D_{2n}}(\tau)| = |D_{2n}| \Rightarrow 2 = 2n$ which is a contradiction.

- Suppose n is even. Notice that, for every integer i,

$$\sigma^{n/2} \circ \underbrace{\sigma^i} = \sigma^{n/2+i} = \underbrace{\sigma^i} \circ \sigma^{n/2} \quad \text{and}$$

$$\sigma^{n/2} \circ \underbrace{\sigma^i \circ \tau} = \sigma^i \circ \sigma^{n/2} \circ \tau = \underbrace{\sigma^i \circ \tau} \circ \sigma^{n/2}. \quad \text{Hence}$$

$\sigma^{n/2} \in Z(D_{2n})$. (I)

Since $|C_{D_{2n}}(\tau)| = 4 \neq 2n$, $C_{D_{2n}}(\tau) \neq D_{2n}$. Thus $\tau \notin Z(D_{2n})$. (II)

Because $Z(D_{2n})$ is a subgroup of D_{2n}, by (I) and (II) $\sigma^{n/2} \circ \tau \notin Z(D_{2n})$. (III)

Since $Z(D_{2n}) \subseteq C_{D_{2n}}(\tau) = \{id., \tau, \sigma^{n/2}, \sigma^{n/2} \circ \tau\}$, $id, \sigma^{n/2} \in Z(D_{2n})$, $\tau \notin Z(D_{2n})$, and $\sigma^{n/2} \circ \tau \notin Z(D_{2n})$, we conclude that $Z(D_{2n}) = \{id., \sigma^{n/2}\}$. $\blacksquare$