Centar. Centralizator. Normalizator.

Definicija (centar grupe)

Centar, $Z(G)$, grupe G je podskup elemenata iz G koji komutiraju sa svakim elementom grupe G. Simbolima

$$Z(G) = \{a \in G \mid ax = xa \text{ za sve } x \in G\}.$$

Oznaka $Z(G)$ dolazi iz činjenice da je njemačka riječ za centar Zentrum. Termin je započeo upotrebljavati J. A. de Séguier 1904.

(#) Pokazati da je $Z(G) = G$ ako i samo ako je G Abelova.

Rj.

„$\Leftarrow$" Pretpostavimo da je G Abelova grupa.

Tada je $ab = ba \quad \forall a, b \in G$. Drugim riječima

$$\{a \in G \mid ax = xa \quad \forall x \in G\} = G$$

$$\Rightarrow \quad Z(G) = G$$

„$\Rightarrow$" Pretpostavimo da je $Z(G) = G$. Drugim riječima

$$\{a \in G \mid ax = xa \quad \forall x \in G\} = G$$

$$\Rightarrow \quad ab = ba \quad \forall a, b \in G \quad \Rightarrow \quad G \text{ je abelova grupa.}$$

(#) Pokazati da je $Z(S_n) = \{id\}$ ako je $n \geq 3$.

Rj:

Pokazaćemo da za bilo koje $\alpha \in S_n$, $\alpha \neq id$, uvijek postoji $\beta \in S_n$ takva da $\alpha\beta \neq \beta\alpha$.

Pa neka je $\alpha \in S_n$, $\alpha \neq id$. Tada postoji i $(1 \leq i \leq n)$ takav da $\alpha(i) = j$ za neki $j \in \{1, 2, .., n\}$, $j \neq i$.

S obzirom da imamo grupu S_n, to postoji $\beta \in S_n$ t.d. $\beta(i) = i$ i $\beta(j) = k$ gdje je $k \neq i$, $k \neq j$ (brojevi i, j, k parbroje s obzirom da je $n \geq 3$).

Sad imamo

$$\left.\begin{aligned} (\alpha\beta)(i) &= \alpha(\beta(i)) = \alpha(i) = j \\ (\beta\alpha)(i) &= \beta(\alpha(i)) = \beta(j) = k \end{aligned}\right\} \overset{j \neq k}{\Rightarrow} (\alpha\beta)(i) \neq (\beta\alpha)(i)$$

$$\Downarrow$$

$$\alpha\beta \neq \beta\alpha$$

Prema tome $Z(S_n) = \{id\}$.

Teorem (centar je podgrupa)

Centar grupe G je podgrupa grupe G.

(#) Dokazati teorem iznad.

Rj:

Skica dokaza:

U dokazu ćemo upotrebiti sljedeći teorem
Neka je G grupa, i neka je H neprazan podskup grupe G.
Ako je $ab \in H$ za sve $a, b \in H$ i ako je $a^{-1} \in H$ za sve $a \in H$
tada je H podgrupa grupe G.

$e \in Z(G) \Rightarrow Z(G) \neq \emptyset$

$a, b \in Z(G) \Rightarrow (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab) \quad \forall x \in G$

$\Rightarrow ab \in Z(G)$

$a \in Z(G) \Rightarrow ax = xa \quad \forall x \in G$

Želimo pokazati da $a^{-1}x = xa^{-1} \quad \forall x \in G$

$ax = xa \Rightarrow a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$

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

$exa^{-1} = a^{-1}xe$

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

$\Rightarrow a^{-1} \in Z(G) \quad \forall a \in G$

(#) Prisjetimo se da se Dihedralna grupa D_n (reda $2n$) može generisati rotacijom $R_{360/n}$ (reda n) i refleksijom F (reda 2) za koje vrijedi da je $FR_{360/n}F = R_{360/n}^{-1}$.
Odrediti $Z(D_n)$ za proizvoljan $n \geq 3$.

Rj.
Prvo primjetimo da je svaka rotacija iz D_n stepen od $R_{360/n} \Rightarrow$ rotacije komutiraju sa rotacijama.

Sada posmatrajmo kada rotacije komutiraju sa refleksijom.
Neka je R bilo koja rotacija iz D_n i neka je F neka refleksija iz D_n.

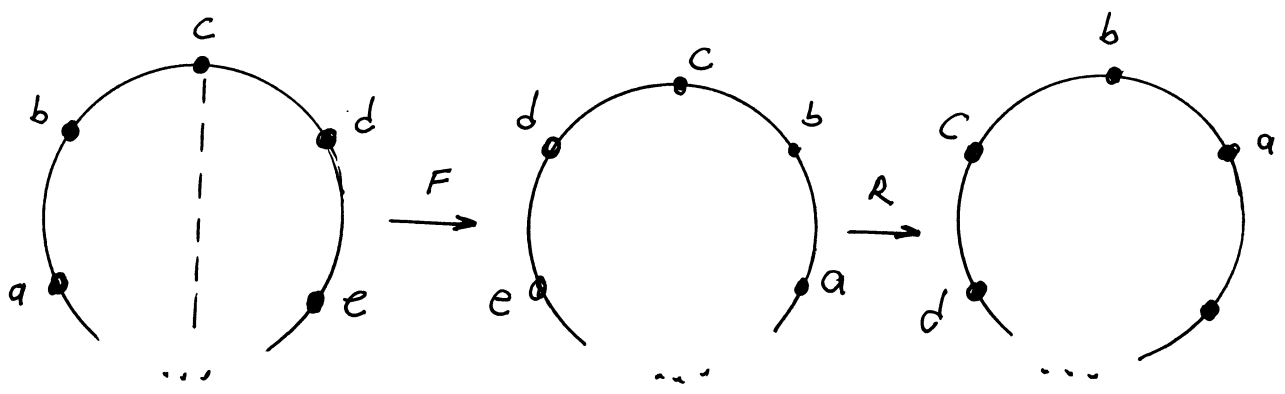
Primjetimo da, s obzirom da je RF refleksija imamo da $RF = (RF)^{-1} = F^{-1}R^{-1} = FR^{-1} \Rightarrow R$ i F komutiraju akko $FR = RF = FR^{-1}$.

$\Updownarrow$

$R = R^{-1}$

$\Downarrow$

$R = R_0$ ili $R = R_{180}$



Rotacija R_{180} je u grupi D_n samo kada je n parno. Prema tome

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\}, & n \text{ parno} \\ \{R_0\}, & \text{kada je } n \text{ neparno.} \end{cases}$$

(#) Neka je G grupa. Pokazati da je tada $Z(G) \trianglelefteq G$, tj. $Z(G)$ je normalna podgrupa grupe G.

R.j. Prvo primjetimo da $Z(G) \neq \emptyset$, s obzirom da je $e \in Z(G)$. Sad neka su $x, y \in Z(G)$ i neka je $g \in G$. Tada

$$gx = xg$$

$$x^{-1}gx = g$$

$$x^{-1}g = gx^{-1}$$

$$x^{-1}gy = gx^{-1}y$$

$$x^{-1}yg = gx^{-1}y \quad \overset{g \text{ proizvoljan}}{\Longrightarrow} \quad x^{-1}y \in Z(G)$$

$$\Downarrow$$

$Z(G)$ je podgrupa grupe G.

U prethodnoj teoremi smo već pokazali da je $Z(G)$ podgrupa grupe G. Ovdje smo dali dokaz na II način.

S obzirom da je za svaki element $h \in Z(G)$

$$ah = ha \quad \forall a \in G$$

to je $\quad aZ(G) = Z(G)a \quad \forall a \in G$

$$\Rightarrow \quad Z(G) \trianglelefteq G.$$

Definicija (centralizator elementa a u grupi G)

Neka je a fiksiran element grupe G. Centralizator elementa a u grupi G, $C(a)$, je skup svih elemenata iz grupe G koji komutiraju sa a. Simbolima

$$C(a) = \{ g \in G \mid ga = ag \}.$$

(#) Pretpostavimo da je G grupa definisana sljedećom Cayley-evom tabelom.

	I	A	B	AB	BA	ABA
I	I	A	B	AB	BA	ABA
A	A	I	AB	B	ABA	BA
B	B	BA	I	ABA	A	AB
AB	AB	ABA	A	BA	I	B
BA	BA	B	ABA	I	AB	A
ABA	ABA	AB	BA	A	B	I

(a) Izračunati $Z(G)$

(b) Izračunati $C(A)$ i $C(AB)$.

R.j.

(a) Iz Cayleyeve tabele primjetimo da $II = I = II$,

$IA = A = AI$,

$IB = B = BI$,

$I(AB) = AB = (AB)I$,

$I(BA) = BA = (BA)I$,

$I(ABA) = ABA = (ABA)I$, $\Rightarrow$ $I \in Z(G)$.

Također, iz Cayleyeve tabele primjetimo da

$AB \neq BA \Rightarrow A \notin Z(G),\ B \notin Z(G)$

$(AB)B = A \neq ABA = B(AB) \Rightarrow AB \notin Z(G)$

$(BA)A = B \neq A(BA) \Rightarrow BA \notin Z(G)$

$(ABA)A = AB \neq BA = A(ABA) \Rightarrow ABA \notin Z(G)$

Možemo zaključiti $Z(G) = \{I\}$.

(b) Iz Cayleyeve tabele vidimo da

$$IA = AI$$

$$AA = AA$$

$$AB \neq BA$$

$$A(AB) \neq (AB)A$$

$$A(BA) \neq (BA)A$$

$$A(ABA) \neq (ABA)A$$

$$\Rightarrow \quad C(A) = \{I, A\}$$

S druge strane imamo da

$$I(AB) = (AB)I$$

$$(BA)(AB) = (AB)(BA)$$

$$(AB)(AB) = (AB)(AB)$$

$$(AB)A \neq A(AB)$$

$$(AB)B \neq B(AB)$$

$$(AB)(ABA) \neq (ABA)(AB)$$

$$\Rightarrow \quad C(AB) = \{I, AB, BA\}.$$

(#) Upotrebiti Cayleyevu tablu Dihedralne grupe D_4, koju smo imali u jednom od prethodnih zadataka, i odrediti $C(a)$ za $\forall a \in D_4$.

Rj:

$$C(R_0) = D_4 = C(R_{180})$$

$$C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270})$$

$$C(H) = \{R_0, H, R_{180}, V\} = C(V)$$

$$C(D) = \{R_0, D, R_{180}, D'\} = C(D').$$

Primjetimo da su svi centralizatori iz ovog primjera u stvari podgrupe grupe D_4. Sljedeća teorema pokazuje da ovo nije slučajno.

Teorem ($C(a)$ je podgrupa)

Za svaki element a grupe G, centralizator elementa a je podgrupa grupe G.

(#) Dokazati teoremu iznad.

Definicija (centralizator skupa S, normalizator skupa S)

Neka je G grupa, i neka je $S \subseteq G$. Podskup

$$C_G(S) = \{g \in G \mid gs = sg \quad \forall s \in S\}$$

grupe G nazivamo centralizator skupa S.

Podskup

$$N_G(S) = \{g \in G \mid gS = Sg\}$$

grupe G nazivamo normalizator skupa S u grupi G.

Primjetimo da je $C_G(S)$ skup svih elemenata grupe G koji komutiraju sa svakim elementom skupa S.

Teorema

Neka je G grupa i neka je $A \subseteq G$. Tada su $C_G(A)$ i $N_G(A)$ podgrupe grupe G.

(#) Dokazati teoremu iznad.

Rj:

Pokažimo da je $C_G(A)$ podgrupa grupe G. Prvo primjetimo da je $C_G(A) \neq 0$ s obzirom da je $1 \in C_G(A)$: prema definiciji identiteta imamo da je $1a = a1 \ \forall a \in G$ (a time i za $\forall a \in A$) pa 1 zadovoljava uslov iz definicije za pripadanje skupu $C_G(A)$.

Sad, pretpostavimo da $x, y \in C_G(A)$ tj. $\forall a \in A \quad xa = ax$ i $ya = ay$ (primjetimo da ovo ne znači da vrijedi $xy = yx$).

$$ya = ay \Rightarrow yay^{-1} = a \Rightarrow ay^{-1} = y^{-1}a \Rightarrow y^{-1} \in C_G(A)$$

$\Rightarrow C_G(A)$ je zatvoren u odnosu na uzimanje inverza.

Sad

$$(xy)a(xy)^{-1} = (xy)a(y^{-1}x^{-1}) =$$

$$= x(yay^{-1})x^{-1} = \left| \begin{array}{l} y \in C_G(A) \\ ya = ay \Rightarrow yay^{-1} = a \end{array} \right|$$

$$= xax^{-1} \underset{a}{\overset{x \in C_G(A)}{=}}$$

$\Rightarrow (xy)a = a(xy) \Rightarrow xy \in C_G(A)$ a time je $C_G(A)$ zatvoren u odnosu na operaciju množenja.

Prema tome $C_G(A) \leq G$.

Slično se pokaže da je $N_G(A) \leq G$.

(#) Provjeriti da li je $Z(G) = C_G(G)$.

Rj.:

$$Z(G) = \{ g \in G \mid gx = xg \text{ za } \forall x \in G \}$$

$A \subseteq G$

$$C_G(A) = \{ g \in G \mid ga = ag \text{ za } \forall a \in A \}$$

$$\Downarrow$$

$$C_G(G) = \{ g \in G \mid gx = xg \text{ za } \forall x \in G \}$$

Da, vrijedi da je $Z(G) = C_G(G)$.

(#) Provjeriti da li je $C_G(A) \leq N_G(A)$

Rj.:

$$g \in C_G(A) \Rightarrow ga = ag \ \forall a \in A \Rightarrow gA = Ag$$

$$\Rightarrow g \in N_G(A).$$

Kako je $C_G(A) \subseteq N_G(A)$ i kako su $C_G(A)$ i $N_G(A)$ grupe to vrijedi da je $C_G(A) \leq N_G(A)$.

(#) Neka je G abelova grupa i neka je $A \subseteq G$. Odredi $C_G(A)$ i $N_G(A)$.

Rj.

G Abelova $\Rightarrow$ $ab = ba$ $\forall a, b \in G$

$A \subseteq G$, $\forall a \in A$ $\quad gag^{-1} = gg^{-1}a = a$

$ga = ag$ $\forall g \in G$

Prema tome $N_G(A) = C_G(A) = G$ za $\forall A \subseteq G$.

(#) Neka je D_4 dihedralna grupa reda 8. i neka je $A = \{R_0, R_{90}, R_{180}, R_{270}\}$. Bez upotrebe Cayleyeve tablice odredi:

(a) $C_{D_4}(A)$;

(b) $N_{D_4}(A)$.

Ako znamo da je $D_4 = \langle R_{90}, H \rangle$ gdje je $R_{90} H R_{90} = H$

Rj.

(a) $C_{D_4}(A) = A$

(b) $N_{D_4}(A) = D_4$.

(#) Neka je $G = S_3$ i neka je $A = \{id, (12)\}$. Izračunaj $C_{S_3}(A)$ i $N_{S_3}(A)$.

(5) Find an element in $C(\alpha)$ that is not in $\langle \alpha \rangle$.

Solution. Since disjoint cycles commute, anything disjoint from α will be in $C(\alpha)$. So, for instance, $(25) \in C(\alpha)$. Moreover $(25) \notin \langle \alpha \rangle = \{\varepsilon, (134), (143)\}$. □

(6) Suppose that G is a group and $a \in G$. Suppose further that $|a| = 5$. Prove that $C(a) = C(a^3)$.

Solution. First we will show that $C(a) \subseteq C(a^3)$. Suppose that $g \in C(a)$, so that $ga = ag$. We must show that $ga^3 = a^3 g$. Now observe that

$$\begin{aligned} ga^3 &= gaaa && \text{(definition of } a^3\text{)} \\ &= agaa && \text{(since } ga = ag\text{)} \\ &= aaga && \text{(since } ga = ag\text{)} \\ &= aaag && \text{(since } ga = ag\text{)} \\ &= a^3 g && \text{(definition of } a^3\text{).} \end{aligned}$$

Hence we have $g \in C(a^3)$, as desired.

Now we show that $C(a^3) \subseteq C(a)$. For this, suppose that $g \in C(a^3)$, so that $ga^3 = a^3 g$. Observe that

$$\begin{aligned} ga &= gae && \text{(definition of } e\text{)} \\ &= gaa^5 && \text{(since } |a| = 5\text{)} \\ &= ga^6 && \text{(exponent arithmetic)} \\ &= ga^3 a^3 && \text{(exponent arithmetic)} \\ &= a^3 ga^3 && \text{(since } g \in C(a^3)\text{)} \\ &= a^3 a^3 g && \text{(since } g \in C(a^3)\text{)} \\ &= a^6 g && \text{(exponent arithmetic)} \\ &= a^5 ag && \text{(exponent arithmetic)} \\ &= eag && \text{(since } |a| = 5\text{)} \\ &= ag && \text{(definition of } e\text{).} \end{aligned}$$

Hence $g \in C(a)$, as desired. □

(2) Recall that for an element $a \in G$, we define $\varphi_a \in \text{Inn}(G)$ by $\varphi_a(x) = axa^{-1}$. Prove that $\varphi_h = \varphi_g$ if and only if $g^{-1}h \in Z(G)$.

Solution. Observe that $\varphi_h = \varphi_g$ if and only if, for all $x \in G$, we have $\varphi_h(x) = \varphi_g(x)$. Based on the definition of inner automorphisms, this condition holds if and only, for all $x \in G$, we have $hxh^{-1} = gxg^{-1}$. By multiplying on the left by g^{-1} and the right by h, this condition holds if and only if, for all $x \in G$, we have $g^{-1}hx = xg^{-1}h$. But this latter condition is precisely the definition of $g^{-1}h \in Z(G)$. □

▮ Theorem 9.3 *G/Z* Theorem

Let G be a group and let Z(G) be the center of G. If G/Z(G) is cyclic, then G is Abelian.

PROOF Since G is Abelian is equivalent to $Z(G) = G$, it suffices to show that the only element of $G/Z(G)$ is the identity coset $Z(G)$. To this end, let $G/Z(G) = \langle gZ(G) \rangle$ and let $a \in G$. Then there exists an integer i such that $aZ(G) = (gZ(G))^i = g^iZ(G)$. Thus, $a = g^iz$ for some z in $Z(G)$. Since both g^i and z belong to $C(g)$, so does a. Because a is an arbitrary element of G this means that every element of G commutes with g so $g \in Z(G)$. Thus, $gZ(G) = Z(G)$ is the only element of $G/Z(G)$. ▮

A few remarks about Theorem 9.3 are in order. First, our proof shows that a better result is possible: If G/H is cyclic, where H is a subgroup of $Z(G)$, then G is Abelian. Second, in practice, it is the contrapositive of the theorem that is most often used—that is, if G is non-Abelian, then $G/Z(G)$ is not cyclic. For example, it follows immediately from this statement and Lagrange's Theorem that a non-Abelian group of order pq, where p and q are primes, must have a trivial center. Third, if $G/Z(G)$ is cyclic, it must be trivial.

(3) Suppose that $|G| = p^3$ and that $Z(G) \neq \{e\}$ and $Z(G) \neq G$. Prove that $Z(G) \approx \mathbb{Z}_p$.

Solution. By Lagrange's theorem we know that $|Z(G)| \in \{1, p, p^2, p^3\}$. Now if $|Z(G)| = 1$ then $Z(G) = \{e\}$, which we've ruled out; hence $|Z(G)| \neq 1$. Likewise if $|Z(G)| = p^3$ then G is abelian, another scenario we know doesn't hold by assumption; hence $|Z(G)| \neq p^3$. Hence the only possibilities are $|Z(G)| = p$ or $|Z(G)| = p^2$.

We'll rule out the possibility that $|Z(G)| = p^2$. To see this is impossible, assume for contradiction's sake that $|Z(G)| = p^2$. It therefore follows that $|G/Z(G)| = p^3/p^2 = p$. But then Corollary 3 on page 138 tells us that $G/Z(G) \approx \mathbb{Z}_p$. But if this is the case then $G/Z(G)$ is cyclic, and so it follows that G is abelian. This contradicts our assumption that G is not abelian. Hence we cannot have $|Z(G)| = p^2$.

By process of elimination, we have $|Z(G)| = p$. By the corollary to Lagrange's theorem, we have $Z(G) \approx \mathbb{Z}_p$. □

(2) Suppose that G is a group so that $[G : Z(G)] \leq 3$. Prove that G is abelian.

Solution. Recall that $[G : Z(G)]$ is defined to be the number of left cosets of $Z(G)$ in G, and hence we have $[G : Z(G)] = |G/Z(G)|$. Now if $[G : Z(G)] = 1$, this means that G/H is a group with one element. But there is — up to isomorphism — only one group with a single element: $\mathbb{Z}_1$. Hence if $[G : Z(G)] = 1$, then $G \simeq \mathbb{Z}_1$.

On the other hand, if $[G : Z(G)] = 2$, then $G/Z(G)$ is a group with 2 elements. Since 2 is a prime, a corollary to Lagrange's theorem tells us that $G/Z(G) \simeq \mathbb{Z}_2$. Similarly, if $[G : Z(G)] = 3$, then $G/Z(G)$ is a group with 3 elements, and then the primeness of 3 tells us that $G/Z(G) \simeq \mathbb{Z}_3$.

Since $\mathbb{Z}_n$ is cyclic for any $n \geq 1$, then in all of these three cases we see that $G/Z(G)$ is cyclic. But then the G/Z theorem tells us that G is abelian, as desired.

[Note: it might be tempting to write $[G : Z(G)] = |G|/|Z(G)|$, and this is certainly true when G is finite. But when G is infinite, the quantity $|G|/|Z(G)|$ is not well-defined. Other bizarre things can happen if you try to do order-based arguments and $|G| = \infty$. For instance, if $[G : Z(G)] = 1$ you can (correctly) deduce that $|G| = |Z(G)|$. However, if $|G| = \infty$, this is not enough to then deduce that $G = Z(G)$ (so that G is abelian); for example, the group $G = \mathrm{GL}_n(\mathbb{R})$ has $|G| = \infty$ and $|Z(G)| = \infty$, and yet $G \neq Z(G)$. Said another way: the equality $[G : Z(G)] = 1$ tells us more than just $|G| = |Z(G)|$, and we need that "extra information" when G is infinite to make a sound argument.

Fortunately, if one simply sticks with the definition $[G : Z(G)] = |G/Z(G)|$, one can present a uniform argument in which groups of infinite order to present any real subtleties.] $\square$

7. Let G be a finite group and p, q be two primes not necessarily distinct.

   (a) The *center* $Z(G)$ of G is the set of elements that commute with the whole group G.

   $$i.e. \quad Z(G) = \{z \in G \mid zg = gz, \ \forall g \in G\}.$$

   Show that this is a normal subgroup of G.

   (b) If $|G| = pq$ then either G is abelian or $Z(G) = 1$. (Textbook §3.2 Problem 4.)

Proof. (a) Let $g \in G$ be any element. We want to show that $gZ(G)g^{-1} = Z(G)$. Let $a \in Z(G)$ be any element. Then $gag^{-1}gg^{-1}a = a \in Z(G)$, as wanted.

(b) If $Z(G)$ is not 1, then $Z(G)$ is a normal subgroup of G, hence must have order dividing pq, i.e. p, q or pq. If $|Z(G)| = pq$, then G is abelian, as wanted.

Assume, without loss of generality, that $|Z(G)| = p$. But then $G/Z(G)$ has order q, also a prime, so must be cyclic, say with generator g. Let g_1, g_2 be any two elements in G. Then $g_1 = g^a z_1$, $g_2 = g^b z_2$ with $z_1, z_2 \in Z(2)$. But then it's clear that $g_1 g_2 = g_2 g_1 = g^{a+b} z_1 z_2$, so any two elements of G commute. This would contradict the assumption that $|Z(G)| = p$.

Alternatively, if we want to avoid using the fact that the quotient $G/Z(G)$ is a subgroup, we can choose any nonidentity coset of $Z(G)$, say $gZ(G)$. Then $g \notin Z(G)$. Note that the subgroup generated by g and $Z(G)$ must be all of G, for there are no intermediate subgroups between $Z(G)$ and G (if H was such a subgroup, then $q = [G : Z(G)]$ would equal $[H : Z(G)] \cdot [G : H]$. But q is prime, hence either $H = Z(G)$ or $H = G$).

This means that every element can be written as $g^a z$ for some integer a and $z \in Z(G)$ (a general element of the subgroup generated by g and $Z(G)$ is a product $g^{a_1} z_1 g^{a_2} z_2 \cdots$, but since z_i commute with everything in G, such an element can be rewritten as $g^a z$).

□

Examples

(1) If G is abelian then all the elements of G commute, so $Z(G) = G$. Similarly, $C_G(A) = N_G(A) = G$ for *any* subset A of G since $gag^{-1} = gg^{-1}a = a$ for every $g \in G$ and every $a \in A$.

(2) Let $G = D_8$ be the dihedral group of order 8 with the usual generators r and s and let $A = \{1, r, r^2, r^3\}$ be the subgroup of rotations in D_8. We show that $C_{D_8}(A) = A$. Since all powers of r commute with each other, $A \leq C_{D_8}(A)$. Since $sr = r^{-1}s \neq rs$ the element s does not commute with all members of A, i.e., $s \notin C_{D_8}(A)$. Finally, the elements of D_8 that are not in A are all of the form sr^i for some $i \in \{0, 1, 2, 3\}$. If the element sr^i were in $C_{D_8}(A)$ then since $C_{D_8}(A)$ is a *subgroup* which contains r we would also have the element $s = (sr^i)(r^{-i})$ in $C_{D_8}(A)$, a contradiction. This shows $C_{D_8}(A) = A$.

(3) As in the preceding example let $G = D_8$ and let $A = \{1, r, r^2, r^3\}$. We show that $N_{D_8}(A) = D_8$. Since, in general, the centralizer of a subset is contained in its normalizer, $A \leq N_{D_8}(A)$. Next compute that

$$sAs^{-1} = \{s1s^{-1},\ srs^{-1},\ sr^2s^{-1},\ sr^3s^{-1}\} = \{1,\ r^3,\ r^2,\ r\} = A,$$

so that $s \in N_{D_8}(A)$. (Note that the *set* sAs^{-1} equals the *set* A even though the elements in these two sets appear in different orders — this is because s is in the normalizer of A but not in the centralizer of A.) Now both r and s belong to the *subgroup* $N_{D_8}(A)$ and hence $s^ir^j \in N_{D_8}(A)$ for all integers i and j, that is, every element of D_8 is in $N_{D_8}(A)$ (recall that r and s *generate* D_8). Since $D_8 \leq N_{D_8}(A)$ we have $N_{D_8}(A) = D_8$ (the reverse containment being obvious from the definition of a normalizer).

(4) We show that the center of D_8 is the subgroup $\{1, r^2\}$. First observe that the center of any group G is contained in $C_G(A)$ for any subset A of G. Thus by Example 2 above $Z(D_8) \leq C_{D_8}(A) = A$, where $A = \{1, r, r^2, r^3\}$. The calculation in Example 2 shows that r and similarly r^3 are not in $Z(D_8)$, so $Z(D_8) \leq \{1, r^2\}$. To show the reverse inclusion note that r commutes with r^2 and calculate that s also commutes with r^2. Since r and s generate D_8, every element of D_8 commutes with r^2 (and 1), hence $\{1, r^2\} \leq Z(D_8)$ and so equality holds.

(5) Let $G = S_3$ and let A be the subgroup $\{1,\ (1\,2)\}$. We explain why $C_{S_3}(A) = N_{S_3}(A) = A$. One can compute directly that $C_{S_3}(A) = A$, using the ideas in Example 2 above to minimize the calculations. Alternatively, since an element commutes with its powers, $A \leq C_{S_3}(A)$. By Lagrange's Theorem (Exercise 19 in Section 1.7) the order of the subgroup $C_{S_3}(A)$ of S_3 divides $|S_3| = 6$. Also by Lagrange's Theorem applied to the subgroup A of the group $C_{S_3}(A)$ we have that $2 \mid |C_{S_3}(A)|$. The only possibilities are: $|C_{S_3}(A)| = 2$ or 6. If the latter occurs, $C_{S_3}(A) = S_3$, i.e., $A \leq Z(S_3)$; this is a contradiction because $(1\,2)$ does not commute with $(1\,2\,3)$. Thus $|C_{S_3}(A)| = 2$ and so $A = C_{S_3}(A)$.

Next note that $N_{S_3}(A) = A$ because $\sigma \in N_{S_3}(A)$ if and only if

$$\{\sigma 1\sigma^{-1},\ \sigma(1\,2)\sigma^{-1}\} = \{1,\ (1\,2)\}.$$

Since $\sigma 1\sigma^{-1} = 1$, this equality of sets occurs if and only if $\sigma(1\,2)\sigma^{-1} = (1\,2)$ as well, i.e., if and only if $\sigma \in C_{S_3}(A)$.

The center of S_3 is the identity because $Z(S_3) \leq C_{S_3}(A) = A$ and $(1\,2) \notin Z(S_3)$.

Lemma 8.18. *Let H be a subgroup of a group G. Then for any $x \in G$*

$$N_G(x^{-1}Hx) = x^{-1}N_G(H)x.$$

Proof: For any $g \in N_G(H)$, we have

$$\begin{aligned} x^{-1}gx \cdot x^{-1}Hx &= x^{-1}gHx \\ &= x^{-1}Hgx \\ &= x^{-1}Hx \cdot x^{-1}gx \end{aligned}$$

Therefore

$$x^{-1}N_G(H)x \subseteq N_G(x^{-1}Hx) \tag{8.1}$$

Taking $x^{-1}Hx$ for H, we get from 8.1

$$xN_G(x^{-1}Hx)x^{-1} \subseteq N_G(x(x^{-1}Hx)x^{-1}) = N_G(H)$$

Therefore

$$N_G(x^{-1}Hx) \subseteq x^{-1}N_G(H)x \tag{8.2}$$

Now, from 8.1 and 8.2, we conclude

$$x^{-1}N_G(H)x = N_G(x^{-1}Hx)$$ ■

7.5.3 *Lemma*

Let π be a permutation. Then

$$(*)\ \pi(a_1a_2...a_k)\pi^{-1} = (\pi(a_1)\ \pi(a_2)..\pi(a_k))\,.$$

Proof. Applying the left-hand side of equation above to $\pi(a_1)$, we get

$$\pi(a_1a_2...a_k)\pi^{-1}\,[\,\pi(a_1)\,] = \pi(a_1a_2...a_k)[a_1] = \pi(a_2)\,.$$

In general, applying the left-hand side to $\pi(a_j)$, $j<k$, we get $\pi(a_{j+1})$ and when $j=k$,

$$\pi(a_1a_2...a_k)\pi^{-1}[\pi(a_k)] = \pi(a_1a_2...a_k)[a_k] = \pi(a_1).$$

Therefore, one of the nontrivial cycles of the permutation $\pi(a_1a_2...a_k)\pi^{-1}$ is $(\pi(a_1)\ \pi(a_2)....\pi(a_k))$.

The permutation on the right-hand side of (*) moves the symbols $\pi(a_j)$, $1 \le j \le k$ and no others. We need only show that the same is true of $\pi(a_1a_2...a_k)\pi^{-1}$ and the result will be proved. Suppose

$$b \notin \{\pi(a_1), \pi(a_2), ..., \pi(a_k)\}\,.$$

Then $\pi^{-1}(b) \notin \{a_1, a_2, ..., a_k\}$ (why?). Hence $(a_1a_2...a_k)[\pi^{-1}(b)] = \pi^{-1}(b)$ and so

$$\pi(a_1a_2....a_k)\pi^{-1}[b] = \pi\{(a_1a_2....a_k)[\pi^{-1}(b)]\} = \pi\pi^{-1}(b) = b\,.\blacksquare$$

Since the relation '~' is reflexive, $S \in C(S)\ \forall\ S(\neq \phi) \subseteq G$

Also, $C(S) \subseteq P(G)\ \forall\ S(\neq \phi) \subseteq G$,

where P(G) is the set of all non-empty subsets of G.

$$\therefore \quad P(G) = \bigcup_{S(\neq\phi)\subseteq G} \{S\} \subseteq \bigcup_{S(\neq\phi)\subseteq G} C(S) \subseteq P(G)$$

$$\therefore \quad P(G) = \bigcup_{S(\neq\phi)\subseteq G} C(S).$$

In particular, let G be a finite group and

$$P(G) = \bigcup_{i=1}^{t} C(S_i), \qquad \textbf{(P(G) is the set of all non-empty subsets of G)}$$

where the equivalence classes $C(S_1), C(S_2), \ldots\ldots, C(S_t)$ are mutually disjoint.

$$\therefore \quad o(P(G)) = \sum_{i=1}^{t} o(C(S_i)).$$

8. NORMALIZER OF A SET *(K.U. 2005)*

Let G be a group and K, a subgroup of G. For $S(\neq \phi) \subseteq G$, the set $\{x \in K : x^{-1}Sx = S\}$ is called the **normalizer** of the set S in K and it is denoted by $N_K(S)$.

In particular, G is a subgroup of G and we have

$$N_G(S) = \{x \in G : x^{-1}Sx = S\}.$$

For simplicity, we write $N_G(S)$ as N(S) and call it as the normalizer of S.

Thus, $N(S) = \{x \in G : x^{-1}Sx = S\}$.

Remark. If G is an abelian group and $S(\neq \phi) \subseteq G$, then $x^{-1}Sx = S \quad \forall\ x \in G$.

$\therefore \quad N(S) = G \quad \forall\ S(\neq \phi) \subseteq G.$

Theorem 1. *Let G be a group. For any non-empty subset S of G, the normalizer N(S) of S is a subgroup of G.* (K.U. 2005)

Proof. We have $N(S) = \{x \in G : x^{-1}Sx = S\}$.

$e \in N(S)$, because $e^{-1}Se = eSe = S$. $\therefore$ N(S) is non-empty.

Let $x, y \in N(S)$. $\therefore\ x^{-1}Sx = S, y^{-1}Sy = S$

Now $(xy)^{-1}\, S(xy) = (y^{-1}x^{-1})\, S(xy) = y^{-1}(x^{-1}Sx)\, y = y^{-1}Sy = S$

$\therefore \quad (xy)^{-1}\, S(xy) = S \qquad \therefore\ xy \in N(S)$

Let $x \in N(S)$. $\therefore\ x^{-1}Sx = S$

$\Rightarrow \quad x(x^{-1}Sx)\, x^{-1} = xSx^{-1} \quad \Rightarrow \quad (xx^{-1})\, S(xx^{-1}) = xSx^{-1} \quad \Rightarrow \quad eSe = xSx^{-1}$

$\Rightarrow \quad xSx^{-1} = S \quad \Rightarrow \quad (x^{-1})^{-1}\, S(x^{-1}) = S$

$\therefore \quad x^{-1} \in N(S)$

$\therefore$ N(S) is a subgroup of G.

Remark. The normalizer N(S) may not be a normal subgroup of G.

Example 10. *Let G be a group and K, a subgroup of G. If $S(\neq \phi) \subseteq G$, then show that $N_K(S)$ is a subgroup of G.*

Sol. We claim that $N_K(S) = N(S) \cap K$.

$$x \in N_K(S) \Leftrightarrow x^{-1}Sx = S \text{ and } x \in K \Leftrightarrow x \in N(S) \text{ and } x \in K$$

$\Leftrightarrow\ x \in N(S) \cap K. \quad \therefore\ N_K(S) = N(S) \cap K.$

Since N(S) is a subgroup of G and the intersection of two subgroups is again a subgroup, the set $N_K(S)$ is also a subgroup of G.

Example 11. *Let H be a subgroup of a group G. Show that H is normal iff N(H) = G.* (M.D.U. 2005)

Sol. Let H be a normal subgroup of the group G.

$\Rightarrow \quad ghg^{-1} \in H \quad \forall\, h \in H, g \in G$

Let $x \in G, \quad h \in H.$

$\therefore \quad x^{-1}hx = x^{-1}h(x^{-1})^{-1} \in H \qquad (\because \quad x^{-1} \in G)$

$\Rightarrow \quad x^{-1}Hx \subseteq H$

Also $\quad h = x^{-1}(xhx^{-1})x \in x^{-1}Hx \qquad (\because \quad xhx^{-1} \in H)$

$\Rightarrow \quad H \subseteq x^{-1}Hx$

$\Rightarrow \quad x^{-1}Hx = H \quad \Rightarrow \quad x \in N(H)$

$\therefore \quad N(H) = G$

Conversely, let $N(H) = G.$

Let $x \in G, h \in H.$

$\Rightarrow \quad x \in N(H) \quad \Rightarrow \quad x^{-1}Hx = H \quad \Rightarrow \quad xx^{-1}Hxx^{-1} = xHx^{-1}$

$\Rightarrow \quad xHx^{-1} = H \quad \Rightarrow \quad xhx^{-1} \in H$

$\therefore$ H is a normal subgroup of G.

Theorem 2. *If G is a finite group and $S(\neq \phi) \subseteq G$ then* $o(C(S)) = \dfrac{o(G)}{o(N(S))}$.

Proof. We have $\quad C(S) = \{x^{-1}Sx : x \in G\}.$

Let A be the set of all right cosets of the subgroup N(S) in G.

Define $\phi : A \to C(S)$ by $\phi(N(S)x) = x^{-1}Sx \quad \forall\, x \in G$

ϕ is well defined. Let $x, y \in G.$

$N(S)x = N(S)y \quad \Rightarrow \quad xy^{-1} \in N(S) \qquad (\because \quad Ha = Hb \quad \Leftrightarrow \quad ab^{-1} \in H)$

$\Rightarrow \quad (xy^{-1})^{-1}\, Sxy^{-1} = S \quad \Rightarrow \quad yx^{-1}\, Sxy^{-1} = S \quad \Rightarrow \quad y^{-1}(yx^{-1}Sxy^{-1})y = y^{-1}Sy$

$\Rightarrow \quad (y^{-1}y)(x^{-1}Sx)y^{-1}y = y^{-1}Sy \quad \Rightarrow \quad x^{-1}Sx = y^{-1}Sy$

$\Rightarrow \quad \phi(N(S)x) = \phi(N(S)y).$

$\therefore \quad \phi$ is well defined.

ϕ is one-one. Let $x, y \in G.$

$\phi(N(S)x) = \phi(N(S)y) \quad \Rightarrow \quad x^{-1}Sx = y^{-1}Sy \quad \Rightarrow \quad y(x^{-1}Sx)y^{-1} = y(y^{-1}Sy)y^{-1}$

$\Rightarrow \quad (yx^{-1})\, S(xy^{-1}) = (yy^{-1})\, S(yy^{-1}) \quad \Rightarrow \quad (xy^{-1})^{-1}\, S(xy^{-1}) = S \quad \Rightarrow \quad xy^{-1} \in N(S)$

$\Rightarrow \quad N(S)x = N(S)y.$

$\therefore \quad \phi$ is one-one.

ϕ is onto. Let $T \in C(S)$

$\therefore \quad \exists\, x \in G : T = x^{-1}Sx.$

Now $N(S)x \in A$ and $\phi(N(S)x) = x^{-1}Sx = T.$

$\therefore \quad \phi$ is onto.

$\therefore$ There is one-to-one correspondence between the right cosets of N(S) in G and the conjugates of S.

Since the group G is finite, we have

$o(C(S))$ = number of elements of C(S)

= number of conjugates of S.

$$= \text{number of right cosets of } N(S) \text{ in } G \qquad (\because \ \phi \text{ is 1–1 and onto})$$

$$= \frac{o(G)}{o(N(S))}$$

$$\therefore \qquad o(C(S)) = \frac{o(G)}{o(N(S))}.$$

In other words, the number of conjugates of S is equal to the index of N(S) in G *i.e.*, $o(C(S)) = [G : N(S)]$.

Example 12. *Let G be a group and S, a subgroup of G. Show that S is a normal subgroup of N(S). Also, N(S) is the largest subgroup of G, in which S is normal.*

Sol. We know that N(S) is a subgroup of the group G.

Let $x \in S$. We claim that $x^{-1}Sx = S$.

$$s \in S \ \Rightarrow \ s = ese = (x^{-1}x)\, s(x^{-1}x) = x^{-1}(xsx^{-1})\, x \in x^{-1}Sx$$

$$(\because \ x, s \in S \ \Rightarrow \ xsx^{-1} \in S)$$

$$\therefore \qquad S \subseteq x^{-1}Sx$$

$$x^{-1}sx \in x^{-1}Sx \ \Rightarrow \ s \in S \ \Rightarrow \ x^{-1}sx \in S \qquad (\because \ x, s \in S \ \Rightarrow \ x^{-1}sx \in S)$$

$$\therefore \qquad x^{-1}Sx \subseteq S$$

Combining, we get $x^{-1}Sx = S$. $\therefore \ x \in N(S)$

$\therefore \quad S \subseteq N(S)$. $\therefore$ S is a subgroup of N(S).

Let $x \in N(S)$ and $s \in S$. $\therefore \ x^{-1}Sx = S$

$$\Rightarrow \quad x(x^{-1}Sx)x^{-1} = xSx^{-1} \ \Rightarrow \ (xx^{-1})S(xx^{-1}) = xSx^{-1} \ \Rightarrow \ eSe = xSx^{-1} \ \Rightarrow \ xSx^{-1} = S$$

$\therefore \quad xsx^{-1} \in S$ $\therefore$ S is a normal subgroup of N(S).

Now let H be any subgroup of G in which S is normal.

We shall show that $H \subseteq N(S)$.

Let $h \in H$.

$\therefore \ hsh^{-1} \in S \ \ \forall \ \ s \in S$

In order to show that $h \in N(S)$, it is sufficient to show that $h^{-1}Sh = S$.

Let $s \in S$. $h \in H$ implies $h^{-1} \in H$.

$\therefore \ h^{-1}s(h^{-1})^{-1} \in S$ *i.e.*, $h^{-1}sh \in S$

$\therefore \quad h^{-1}Sh \subseteq S$

Also, $\qquad s = ese = (h^{-1}h)\, s(h^{-1}h) = h^{-1}(hsh^{-1})\, h \qquad \ldots(1)$

Now $h \in H$, $s \in S$ implies $hsh^{-1} \in S$.

$\therefore \quad h^{-1}(hsh^{-1})h \in h^{-1}Sh$

$\therefore \ (1) \ \Rightarrow \quad s \in h^{-1}Sh$

$\therefore \quad S \subseteq h^{-1}Sh$

Combining, we get $h^{-1}Sh = S$.

$\therefore \quad h \in N(S)$. $\therefore \ H \subseteq N(S)$

$\therefore$ N(S) is the largest subgroup of G in which S is normal.

9. DOUBLE COSET

Let H and K be two (not necessarily distinct) subgroups of a group G and let $x \in G$. The set $\{hxk : h \in H, k \in K\}$ is called a **double coset** of the group G and is denoted by HxK.

Theorem 1. *Let H and K be two (not necessarily distinct) subgroups of a group G. For $x, y \in G$, the double cosets HxK and HyK are either disjoint, or identical.*

12. CENTRALIZER OF A SET (*K.U. 2005*)

Let G be a group. For $S(\neq \phi) \subseteq G$, the set $\{x \in G : x^{-1}sx = s, \forall\, s \in S\}$ is called the **centralizer** of the non-empty subset S of G.

Theorem. *Let G be a group. For any non-empty subset S of G, the centralizer of S is a subgroup of G.* (K.U. 2005)

Proof. Let C be the centralizer of S in G.

$\therefore \quad C = \{x \in G : x^{-1}sx = s, \forall\, s \in S\}$

$e \in C$, because $e^{-1}se = ese = s \quad \forall\, s \in S. \quad \therefore \quad C$ is non-empty.

Let $x, y \in C. \quad \therefore \quad x^{-1}sx = s, y^{-1}sy = s \quad \forall\, s \in S$

Now $\quad (xy)^{-1}s(xy) = (y^{-1}x^{-1})\, s(xy) = y^{-1}(x^{-1}sx)y = y^{-1}sy = s$

$\therefore \quad (xy)^{-1}s(xy) = s \quad \forall\, s \in S \quad \therefore \quad xy \in C$

Let $\quad x \in C. \quad \therefore \quad x^{-1}sx = s \quad \forall\, s \in S$

$\Rightarrow \quad x(x^{-1}sx)x^{-1} = xsx^{-1} \quad \Rightarrow \quad (xx^{-1})s(xx^{-1}) = xsx^{-1}$

$\Rightarrow \quad ese = xsx^{-1} \quad \Rightarrow \quad xsx^{-1} = s \quad \Rightarrow \quad (x^{-1})^{-1}s(x^{-1}) = s$

$\therefore \quad (x^{-1})^{-1}s(x^{-1}) = s \quad \forall\, s \in S \quad \therefore \quad x^{-1} \in C$

$\therefore$ C is a subgroup of G.