Quiz 1

Due: 10:00 a.m. April 18, 2007

Division: **ID#:** **Name:**

1. Let d and e be integers satistying $d \mid e$ and $e \mid d$. Show that $e = d$ or $-d$.

2. Let $a_1, a_2, \ldots, a_n$ be integers and e a common divisor of $a_1, a_2, \ldots, a_n$, i.e., $e \mid a_i$ for $i = 1, 2, \ldots, n$. Show that the following conditions are equivalent.

   (a) $c \mid a_i$ for $i = 1, 2, \ldots, n \Rightarrow c \mid e$.

   (b) There exist integers $x_1, \ldots, x_n$ such that $e = a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

3. Find all elements $[a] \in \boldsymbol{Z}_{24}$ such that there exists $[x] \in \boldsymbol{Z}_{24}$ satisfying $[a][x] = [1]$.

Message: What do you expect from this course? Any requests?

Solutions to Quiz 1

April 18, 2007

1. Let d and e be integers satistying $d \mid e$ and $e \mid d$. Show that $e = d$ or $-d$.

   Sol. Since $d \mid e$ and $e \mid d$, there exist integers a and b such that $e = ad$, $d = be$. Hence if one of d or e is zero, then both are zero, and $e = d$ or $-d$ in this case. Suppose both d and e are nonzero. Since $e = ad$, $d = be$ implies $e = ad = abe$, $1 = ab$. Since both a and b are integers, we have $a = 1$ or -1. Since $e = ad$, $e = d$ or $e = -d$. ■

2. Let $a_1, a_2, \ldots, a_n$ be integers and e a common divisor of $a_1, a_2, \ldots, a_n$, i.e., $e \mid a_i$ for $i = 1, 2, \ldots, n$. Show that the following conditions are equivalent.

   (a) $c \mid a_i$ for $i = 1, 2, \ldots, n \Rightarrow c \mid e$.

   (b) There exist integers $x_1, \ldots, x_n$ such that $e = a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

   Sol. Let $d = \gcd\{a_1, a_2, \ldots, a_n\}$. Then $d \geq 0$ and d satisfies $d \mid a_i$ for $i = 1, 2, \ldots, n$, and (a), (b).

   Suppose e satisfies (a). Then $d \mid e$ by (a), and $e \mid d$ as d satisfies (a) by replacing e by d. Hence by 1, $e = d$ or $-d$. Since d satisfies (b), e satisfies (b) as well.

   Suppose e satisfies (b). Let c be an integer satisfying $c \mid a_i$ for $i = 1, 2, \ldots, n$. Since e has an expression $e = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, $c \mid e$. This shows (a). ■

   The above problem shows that the greatest common divisor of $a_1, a_2, \ldots, a_n$ can also be defined as a nonnegative common divisor of $a_1, a_2, \ldots, a_n$ satisfying (b).

3. Find all elements $[a] \in \boldsymbol{Z}_{24}$ such that there exists $[x] \in \boldsymbol{Z}_{24}$ satisfying $[a][x] = [1]$.

   Sol. Let $U(\boldsymbol{Z}_{24}) = \{[a] \in \boldsymbol{Z}_{24} \mid \text{There exists } [x] \in \boldsymbol{Z}_{24} \text{ such that } [a][x] = [1]\}$. Since $[1] = [a][x] = [ax]$ by the definition of multiplication in $\boldsymbol{Z}_{24}$, $ax \equiv 1 \pmod{24}$. Hence there exists an integer y such that $ax - 1 = 24y$. Hence $ax - 24y = 1$. Let $d = \gcd\{a, 24\}$. Then $d \mid ax - 24y = 1$. So $d = 1$. On the other hand, if $\gcd\{a, 24\} = 1$, there exist integers x and y such that $ax + 24y = 1$. Thus $[a][x] = [1 - 24y] = [1]$. Hence $[a] \in U(\boldsymbol{Z}_{24})$. Therefore

   $$U(\boldsymbol{Z}_{24}) = \{[a] \mid \gcd\{a, 24\} = 1,\ a \in \boldsymbol{Z}\} = \{[1], [5], [7], [11], [13], [17], [19], [23]\}. \quad ■$$

   Of course, you can find elements of $U(\boldsymbol{Z}_{24})$ by brute force. Please note that for all $[a] \in U(\boldsymbol{Z}_{24})$, $[a][a] = [1]$. In general the set of invertible elements in $\boldsymbol{Z}_n$ is denoted by $\boldsymbol{Z}_n^*$. Hence $\boldsymbol{Z}_{24}^* = U(\boldsymbol{Z}_{24})$. It is a well-known fact that

   $$[a][a] = [1] \text{ for all } [a] \in \boldsymbol{Z}_n^* \Leftrightarrow n \mid 24.$$

Quiz 2

Due: 10:00 a.m. April 25, 2007

Division: **ID#:** **Name:**

Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 8 & 1 & 2 & 6 & 3 & 7 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 5 & 6 & 8 & 4 & 2 \end{pmatrix}$.

1. Compute $\pi\sigma\pi^{-1}$.

2. Express each of σ and $\pi\sigma\pi^{-1}$ as a product of disjoint cycles. (Do you recognize some similarity between σ and $\pi\sigma\pi^{-1}$?)

3. Express each of π and σ as a product of transpositions (2-cycles (i, j)). (Is it a shortest?)

4. Express each of π and σ as a product of adjacent transpositions $(1, 2), (2, 3), \ldots, (7, 8)$. (Is it a shortest?)

5. Determine $\text{sign}(\pi)$ and $\text{sign}(\sigma)$.

Message: Any questions, comments or requests?

Solutions to Quiz 2

April 25, 2007

Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 8 & 1 & 2 & 6 & 3 & 7 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 5 & 6 & 8 & 4 & 2 \end{pmatrix}$.

1. Compute $\pi\sigma\pi^{-1}$.

   Sol.

   $$\begin{aligned} &\pi\sigma\pi^{-1} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 8 & 1 & 2 & 6 & 3 & 7 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 5 & 6 & 8 & 4 & 2 \end{pmatrix}\begin{pmatrix} 5 & 4 & 8 & 1 & 2 & 6 & 3 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 1 & 3 & 8 & 7 & 4 & 5 \end{pmatrix}. \end{aligned}$$

2. Express each of σ and $\pi\sigma\pi^{-1}$ as a product of disjoint cycles. (Do you recognize some similarity between σ and $\pi\sigma\pi^{-1}$?)

   Sol.

   $$\begin{aligned} \sigma &= (1,3)(2,7,4,5,6,8), \\ \pi\sigma\pi^{-1} &= (1,2,6,7,4,3)(5,8), \\ (&= (5,8)(4,3,1,2,6,7) = (\pi(1),\pi(3))(\pi(2),\pi(7),\pi(4),\pi(5),\pi(6),\pi(8))). \end{aligned}$$

3. Express each of π and σ as a product of transpositions (2-cycles (i,j)). (Is it a shortest?)

   Sol.

   $$\begin{aligned} \pi &= (1,4)(1,2)(1,5)(3,7)(3,8) \ (= (1,5)(5,2)(2,4)(3,8)(8,7)), \\ \sigma &= (1,3)(2,8)(2,6)(2,5)(2,4)(2,7) \ (= (1,3)(2,7)(7,4)(4,5)(5,6)(6,8)). \end{aligned}$$

   Use the formula in Corollary 3.1.4. Both of these are shortest.

4. Express each of π and σ as a product of adjacent transpositions $(1,2),(2,3),\dots,(7,8)$. (Is it a shortest?)

   Sol.

   $$\begin{aligned} \pi &= (7,8)(4,5)(6,7)(3,4)(4,5)(5,6)(6,7)(2,3)(3,4)(4,5)(1,2)(2,3)(3,4), \\ \sigma &= (6,7)(5,6)(4,5)(5,6)(6,7)(7,8)(2,3)(3,4)(4,5)(5,6)(6,7)(7,8)(1,2)(2,3). \end{aligned}$$

   For the expressions use the formula in Exercise 3.1.4 or consider Amida-Kuji. The minimal number of adjacent transpositions required to express each permutation equals the number ℓ of the permutation to be calculated in the next problem. Can you prove this fact?

5. Determine $\mathrm{sign}(\pi)$ and $\mathrm{sign}(\sigma)$.

   Sol. Since $\ell(\pi) = 13$, $\mathrm{sign}(\pi) = (-1)^{13} = -1$. Similarly since $\ell(\sigma) = (-1)^{14}$, $\mathrm{sign}(\pi) = (-1)^{14} = 1$. Since π is the product of 3 cycles including one 1 cycle, $\mathrm{sign}(\pi) = (-1)^{8-3} = -1$ by Cauchy's Formula in (3.1.9). Similarly σ is the product of 2 cycles, $\mathrm{sign}(\sigma) = (-1)^{8-2} = 1$.

Quiz 3

Due: 10:00 a.m. May 7, 2007

Division: **ID#:** **Name:**

Let $(M, \circ)$ be a monoid with identity element e, i.e., $x \circ e = x = e \circ x$ for all $x \in M$. Let $U = \{x \in M \mid \text{there exist } y, z \in M \text{ such that } x \circ y = e = z \circ x\}$.

1. Suppose $a \circ b = e = c \circ a = a \circ d$ for $a, b, c, d \in M$. Show that $b = c = d$.

2. Show that $e \in U$.

3. Show that if $a, b \in U$, then $a \circ b \in U$.

4. Show that $(U, \circ)$ is a group.

Message: Any requests or questions?

Solutions to Quiz 3

May 7, 2007

Let $(M, \circ)$ be a monoid with identity element e, i.e., $x \circ e = x = e \circ x$ for all $x \in M$. Let $U = \{x \in M \mid \text{there exist } y, z \in M \text{ such that } x \circ y = e = z \circ x\}$.

1. Suppose $a \circ b = e = c \circ a = a \circ d$ for $a, b, c, d \in M$. Show that $b = c = d$.

   Sol. Since

   $$\begin{aligned} b &= e \circ b = (c \circ a) \circ b = c \circ (a \circ b) = c \circ e = c \\ d &= e \circ d = (c \circ a) \circ d = c \circ (a \circ d) = c \circ e = c. \end{aligned}$$

   Hence $b = c = d$. ■

2. Show that $e \in U$.

   Sol. Let $y = z = e$. Then $e \circ e = e = e \circ e$. Hence $e \in M$. ■

3. Show that if $a, b \in U$, then $a \circ b \in U$.

   Sol. By the definition of U, there exist $a', a'', b', b'' \in M$ such that

   $$a \circ a' = e = a'' \circ a, \text{ and } b \circ b' = e = b'' \circ b.$$

   Let $y = b' \circ a'$ and $z = b'' \circ a''$. Then

   $$(a \circ b) \circ y = (a \circ b) \circ (b' \circ a') = a \circ (b \circ (b' \circ a')) = a \circ ((b \circ b') \circ a') = a \circ (e \circ a') = a \circ a' = e.$$

   $$z \circ (a \circ b) = (b'' \circ a'') \circ (a \circ b) = b'' \circ (a'' \circ (a \circ b)) = b'' \circ ((a'' \circ a) \circ b) = b'' \circ (e \circ b) = b'' \circ b = e.$$

   Hence $a \circ b \in U$. ■

4. Show that $(U, \circ)$ is a group.

   Sol. Let $a, b \in U$. Then $a \circ b \in U$ by 3. Hence $U \times U \to U$ $((a, b) \mapsto a \circ b)$ defines a binary operation on U. Since $U \subset M$, for all $a, b, c \in U$, $a \circ (b \circ c) = (a \circ b) \circ c$ and associativity holds. By 2, $e \in U$. Suppose $a \in U$. Then there exists $y, z \in M$ such that $a \circ y = e = z \circ a$. Then by 1, $y = z$ and $y \circ a = e = a \circ y$. Hence $y \in U$ and $(M, \circ)$ is a group. ■

   By 1, we have $U = \{x \in M \mid \text{there exist } y \in M \text{ such that } x \circ y = e = y \circ x\}$. Hence U is the set of invertible elements in M.

Quiz 4

Due: 10:00 a.m. May 14, 2007

Division: **ID#:** **Name:**

1. Let G be a group and a an element of G. Show that a mapping $\ell_a : G \to G (x \mapsto ax)$ is a bijection.

2. Let G be a group and H a nonempty finite subset of G such that $xy \in H$ whenever $x, y \in H$. Show that H is a subgroup of G. (Hint: Let $a \in H$ and consider a mapping $\ell_a : H \to H$ $(x \mapsto ax)$.)

3. Give an example that even if H is a nonempty subset of a group G such that $xy \in H$ whenever $x, y \in H$, H is not a subgroup of G. (Hint: Find such a subset in $(\boldsymbol{Z}, +)$.)

4. Find all subgroups of $(\boldsymbol{Z}_8, +)$. ($[a] + [b] = [a + b]$ for all $a, b \in \boldsymbol{Z}$.)

5. Find all subgroups of $(\boldsymbol{Z}_8^*, \cdot)$ ($\boldsymbol{Z}_8^*$ is the set of invertible elements in a monoid $\boldsymbol{Z}_8$ with respect to the multiplication $[a] \cdot [b] = [ab]$.)

Message: Any questions or requests?

Solutions to Quiz 4

May 14, 2007

1. Let G be a group and a an element of G. Show that a mapping $\ell_a : G \to G\,(x \mapsto ax)$ is a bijection.

   Sol. Suppose $\ell_a(x) = \ell_a(y)$. Then $ax = ay$. By multiplying a^{-1} from the left we have $x = y$. Hence ℓ_a is injective. Let $x \in G$. Then $\ell_a(a^{-1}x) = x$. Hence ℓ_a is surjective. ■

2. Let G be a group and H a nonempty finite subset of G such that $xy \in H$ whenever $x, y \in H$. Show that H is a subgroup of G. (Hint: Let $a \in H$ and consider a mapping $\ell_a : H \to H$ $(x \mapsto ax)$.)

   Sol. Let a be an arbitrary element in H and ℓ_a a mapping $\ell_a : H \to H$ $(x \mapsto ax)$. We can take at least one such a as H is nonempty. By assumption, $ax \in H$ and this mapping is well-defined. By 1 above, this mapping is injective. Since H is a finite set, ℓ_a is bijective. (Note that since ℓ_a is injective, $|H| = |\ell_a(H)|$ and $\ell_a(H) \subset H$.) Since $a \in H$, there is an element $e \in H$ such that $\ell_a(e) = a$. Since $ae = a$, e is the identity element. (This can be seen by multiplying a^{-1} on both hand sides from the left.) Hence $1 \in H$. Since there is also an element $a' \in H$ such that $\ell_a(a') = 1$, $aa' = 1$ implies $a' = a^{-1}$. Thus $a^{-1} \in H$. Therefore H is a subgroup of G by Proposition 4.1 (3,3,3). ■

3. Give an example that even if H is a nonempty subset of a group G such that $xy \in H$ whenever $x, y \in H$, H is not a subgroup of G. (Hint: Find such a subset in $(\boldsymbol{Z}, +)$.)

   Sol. Let $H = \boldsymbol{N}$. With respect to addition, H satisfies the required condition. But H is not a subgroup as the inverse of 1 is not in $\boldsymbol{N}$. ■

4. Find all subgroups of $(\boldsymbol{Z}_8, +)$. ($[a] + [b] = [a + b]$ for all $a, b \in \boldsymbol{Z}$.)

   Sol. $\boldsymbol{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$. Let H be a subgroup of $\boldsymbol{Z}_8$. H must contain $[0]$, the identity element of $\boldsymbol{Z}_8$. If H contains $[1]$, it must contain $[1] + [1] = [2], [1] + [2] = [3], \ldots$ and $H = \boldsymbol{Z}_8$. Similarly, If H contains $[3]$, $[5]$ or $[7]$ then $H = \boldsymbol{Z}_8$. On the other hand, if H contains $[4]$ then $H \supset \{[0], [4]\}$, $[2]$ or $[6]$ then $H \supset \{[0], [6], [4], [2]\}$. Hence if $H \neq \boldsymbol{Z}_8$ or $H \neq \{[0]\}$, H contains $\{[0], [4]\}$ or $\{[0], [2], [4], [6]\}$. It is easy to check that these are subgroups generated by $[4]$ or $[2]$ respectively. Hence these are groups. Moreover, there is no other because if H contains an extra element, then $H = \boldsymbol{Z}_8$. Therefore the following are the list of subgroups of $\boldsymbol{Z}_8$.

   $$\{[0]\},\ \{[0], [4]\},\ \{[0], [2], [4], [6]\}, \boldsymbol{Z}_8. \qquad ■$$

5. Find all subgroups of $(\boldsymbol{Z}_8^*, \cdot)$ ($\boldsymbol{Z}_8^*$ is the set of invertible elements in a monoid $\boldsymbol{Z}_8$ with respect to the multiplication $[a] \cdot [b] = [ab]$.)

   Sol. It is easy to check that $\boldsymbol{Z}_8^* = \{[1], [3], [5], [7]\}$ and $[1]$ is the identity element. Hence subgroups are

   $$\{[1]\},\ \{[1], [3]\},\ \{[1], [5]\},\ \{[1], [7]\}, \boldsymbol{Z}_8^*.$$

   Note that if a subgroup contains both $[3]$ and $[5]$, then it must contain $[3][5] = [7]$ and it must be equal to $\boldsymbol{Z}_8^*$. Other cases are similar. ■

Quiz 5

Due: 10:00 a.m. May 21, 2007

Division: **ID#:** **Name:**

1. Let H be a subgroup of a gourp G. You may use the fact that for a nonempty subset K of a group G, $K \leq G \Leftrightarrow (KK \subseteq K) \wedge (K^{-1} \subseteq K)$.

   (a) For $x, y \in G$, show that $Hx = Hy \Leftrightarrow xy^{-1} \in H$.

   (b) Show that $H = HH = HH^{-1} = H^{-1}$.

   (c) Let K be a nonempty subset of a group G. Show that if $KK^{-1} \subseteq K$ then $K \leq G$.

2. Let $G = \boldsymbol{Z}_{15}$ and $K = \{[0], [5], [25]\} \subseteq \boldsymbol{Z}_{15}$. Show that K is a subgroup of a group G and find all distinct cosets of K in G.

Message: Any questions or requests?

Solutions to Quiz 5

May 21, 2007

1. Let H be a subgroup of a gourp G. You may use the fact that for a nonempty subset K of a group G, $K \leq G \Leftrightarrow (KK \subseteq K) \wedge (K^{-1} \subseteq K)$.

   (a) For $x, y \in G$, show that $Hx = Hy \Leftrightarrow xy^{-1} \in H$.
   Sol. ($\Rightarrow$) Since $1 \in H$, $x = 1x \in Hx = Hy$. Hence there exists $h \in H$ such that $x = hy$. By multiplying y^{-1} from the right, we have $xy^{-1} = h \in H$.
   ($\Leftarrow$) Suppose $xy^{-1} \in H$. Since H is a subgroup of G, $yx^{-1} = (xy^{-1})^{-1} \in H$. Hence

   $$Hx = H(xy^{-1})y \subseteq HHy \subseteq Hy = H(yx^{-1})x \subseteq HHx \subseteq Hx.$$

   Therefore $Hx \subseteq Hy \subseteq Hx$ and so $Hx = Hy$. ■
   It is easy to check that for $x, y \in G$, $xy^{-1} \in H$ defines an equivalence relation on G. Hence another way to show (a) is to check $[x] = Hx$, where $[x] = \{z \in G \mid zx^{-1} \in H\}$, the equivalence class containing x. Note that $x \sim y \Leftrightarrow [x] = [y]$.

   (b) Show that $H = HH = HH^{-1} = H^{-1}$. **Sol.** Since $H \leq G$, $HH \subseteq H$ and $H^{-1} \subseteq H$. Let $h \in H$. Then $h^{-1} \in H$. Hence $h = (h^{-1})^{-1} \in H^{-1} \subseteq H$. Thus $H = H^{-1}$. Since $1 \in H$, for every $h \in H$, $h = h1 \in HH$. Hence $H \subseteq HH$ and $HH = H$. Since $H = H^{-1}$, $H = HH = HH^{-1}$ as desired. ■

   (c) Let K be a nonempty subset of a group G. Show that if $KK^{-1} \subseteq K$ then $K \leq G$.
   Sol. Since K is a nonempty subset of G, there exists an element k in K. Then $1 = kk^{-1} \in KK^{-1} \subseteq K$. Hence $1 \in K$. Let $x, y \in K$. Then $x^{-1} = 1x^{-1} \in KK^{-1} \subseteq K$. Hence $K^{-1} \subseteq K$. Thus $y^{-1} \in K$ and $xy = x(y^{-1})^{-1} \in KK^{-1} \subseteq K$. Therefore $KK \subseteq K$. We have $K \leq G$. ■

2. Let $G = \boldsymbol{Z}_{15}$ and $K = \{[0], [5], [25]\} \subseteq \boldsymbol{Z}_{15}$. Show that K is a subgroup of a group G and find all distinct cosets of K in G.

   Sol. First note that $\boldsymbol{Z}_{15} = \{[0], [1], [2], [3], \ldots, [14]\}$ and $|\boldsymbol{Z}_{15}| = 15$. Moreover, $K = \{[0], [5], [10]\} = \langle [5] \rangle \leq \boldsymbol{Z}_{15}$. By Langrange's Theorem, $|\boldsymbol{Z}_{15} : K| = 15/3 = 5$.

   $$\boldsymbol{Z}_{15}/K = \{K, [1] + K, [2] + K, [3] + K, [4] + K\}.$$

   Note that if $0 \leq i < j \leq 4$, then $0 < j - i < 5$ and $[j] - [i] = [j - i] \notin K$. Hence $[i] + K \neq [j] + K$ by 1 (a). ■

Quiz 6

Due: 10:00 a.m. May 28, 2007

Division: **ID#:** **Name:**

Let N be a subgroup of a group G. Show the following.

1. Let $a \in G$. Then $aN = N = Na$ if and only if $a \in N$.

2. $xNx^{-1} \subseteq N$ for all $x \in G - N \Rightarrow xN = Nx$ for all $x \in G$. ($G - N = \{x \in G \mid x \notin N\}$.)

3. For $x, y \in G$, let $x \sim_G y$ if and only if there exists $g \in G$ such that $y = gxg^{-1}$. Show that $\sim_G$ defines an equivalence relation on G.

4. Show that N is a normal subgroup of G if and only if N is a union of some equivalence classes with respect to $\sim_G$.

5. Let C be an equivalence class with respect to $\sim_G$. Then $|C| = 1$ if and only if every element of C commutes with all elements of G.

Message: Any questions or requests?

Solutions to Quiz 6

May 28, 2007

Let N be a subgroup of a group G. Show the following.

1. Let $a \in G$. Then $aN = N = Na$ if and only if $a \in N$.

   Sol. Suppose $aN = N$. Since $1 \in N$, $a = a1 \in aN = N$, $a \in N$. Suppose $a \in N$. Then

   $$N = aa^{-1}N \subseteq aN^{-1}N \subseteq aN \subseteq NN \subseteq N = Na^{-1}a \subseteq NN^{-1}a \subseteq Na \subseteq N.$$

   Hence $aN = N = Na$. ∎

   This also follows from the following: $bN = aN \Leftrightarrow b^{-1}a \in N$ and $Nb = Na \Leftrightarrow ab^{-1} \in N$ by setting $b = 1$. Conversely if we know Problem 1, then above statements follow immediately as $bN = aN \Leftrightarrow a^{-1}bN = N$ and $Nb = Na \Leftrightarrow N = Nab^{-1}$.

2. $xNx^{-1} \subseteq N$ for all $x \in G - N \Rightarrow xN = Nx$ for all $x \in G$. ($G - N = \{x \in G \mid x \notin N\}$.)

   Sol. Since $xN = Nx$ holds for all $x \in N$ by Problem 1, the hypothesis $xNx^{-1} \subseteq N$ for all $x \in G - N$ is nothing but $xNx^{-1} \subseteq N$ for all $x \in G$. Hence by multiplying x from the right, $xN \subseteq Nx$. Since $xNx^{-1} \subseteq N$ holds for all $x \in G$, it holds for x^{-1} as well. Hence $x^{-1}Nx \subseteq N$, and we have $Nx \subseteq xN$. Therefore, $xN = Nx$ for all $x \in G$. ∎

3. For $x, y \in G$, let $x \sim_G y$ if and only if there exists $g \in G$ such that $y = gxg^{-1}$. Show that $\sim_G$ defines an equivalence relation on G.

   Sol. Let $x \in G$. Then $x = 1x1^{-1}$. Hence $x \sim_G x$. Suppose $x \sim_G y$. Then there exists $g \in G$ such that $y = gxg^{-1}$. We have $x = g^{-1}y(g^{-1})^{-1}$. Since $g^{-1} \in G$, $y \sim_G x$ by definition. Suppose $x \sim_G y$ and $y \sim_G z$. Then there exist $g, g' \in G$ such that $y = gxg^{-1}$ and $z = g'yg'^{-1}$. Hence $z = g'yg'^{-1} = g'gxg^{-1}g'^{-1} = (g'g)x(g'g)^{-1}$. Hence $x \sim_G z$ as $g'g \in G$. Therefore $\sim_G$ is an equivalence relation. ∎

4. Show that N is a normal subgroup of G if and only if N is a union of some equivalence classes with respect to $\sim_G$.

   Sol. Suppose $x \in N$ and $x \sim_G y$. Then there exists $g \in G$ such that $y = gxg^{-1}$. Since N is normal in G, $y = gxg^{-1} \in gNg^{-1} \subseteq N$. Hence if $[x]$ is the equivalence class containing x, $[x] \subseteq N$. Therefore N is a union of equivalence classes. (The equivalence class containing x in this case is often written as x^G, and called the conjugacy class containing x. Therefore a normal subgroup of a group G is a union of conjugacy classes of G.) ∎

5. Let C be an equivalence class with respect to $\sim_G$. Then $|C| = 1$ if and only if every element of C commutes with all elements of G.

   Sol. Suppose $C = \{c\}$. Since $c \sim_G gcg^{-1}$, $gcg^{-1} = c$. Hence $gc = cg$ and c commutes with all elements of G. Conversely if c commutes with all elements of G and $x \sim_G c$, then $x = gcg^{-1}$ for some $g \in G$. But by assumption on c, c commutes with g and $x = c$. Therefore C consists of c only. (The set of elements in G that commutes with all elements of G is called the center of G and denoted by $Z(G)$. Hence $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$. It is easy to see that $Z(G) \lhd G$. Moreover every subgroup H of $Z(G)$ is a normal subgroup of G.) ∎

Quiz 7

Due: 10:00 a.m. June 4, 2007

Division: **ID#:** **Name:**

Let H and K be subgroups of a group G.

1. Show that $H \times K$ becomes a group by the following binary operation. For $(h_1, k_1), (h_2, k_2) \in H \times K$, $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$.

2. Let $\alpha : H \times K \to G$ $((h, k) \mapsto hk)$. Suppose α is a group homomorphism. Show that $hk = kh$ for all $h \in H$ and $k \in K$.

3. For the same mapping α in Problem 2, suppose that α is an injective homomorphism. Show that $H \cap K = 1$.

4. Suppose $HK = G$, $H \cap K = 1$ and both H and K are normal subgroups of G. Then the mapping α in Problem 2 is an isomorphism.

Message: Any questions or requests?

Solutions to Quiz 7

June 4, 2007

Let H and K be subgroups of a group G.

1. Show that $H \times K$ becomes a group by the following binary operation. For $(h_1, k_1), (h_2, k_2) \in H \times K$, $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$.

   Sol. Let $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$. Then

   (i) $((h_1, k_1)(h_2, k_2))(h_3, k_3) = (h_1h_2, k_1k_2)(h_3, k_3) = (h_1h_2h_3, k_1k_2k_3)$
   $= (h_1, k_1)(h_2h_3, k_2k_3) = (h_1, k_1)((h_2, k_2)(h_3, k_3))$.

   (ii) $(h_1, k_1)(1_H, 1_K) = (h_1, k_1) = (1_H, 1_K)(h_1, k_1)$,

   (iii) $(h_1, k_1)(h_1^{-1}, k_1^{-1}) = (1_H, 1_K) = (h_1^{-1}, k_1^{-1})(h_1, k_1)$. Hence $H \times K$ is a group. ■

2. Let $\alpha : H \times K \to G$ $((h, k) \mapsto hk)$. Suppose α is a group homomorphism. Show that $hk = kh$ for all $h \in H$ and $k \in K$.

   Sol. Let $h \in H$ and $k \in K$. Then

   $$hk = \alpha((h, k)) = \alpha((1, k)(h, 1)) = \alpha((1, k))\alpha((h, 1)) = kh.$$

   Hence $hk = kh$ for all $h \in H$ and $k \in K$.

3. For the same mapping α in Problem 2, suppose that α is an injective homomorphism. Show that $H \cap K = 1$.

   Sol. Let $x \in H \cap K$. Since $(x, x^{-1}) \in H \times K$ and

   $$\alpha((1, 1)) = 1 = \alpha((x, x^{-1}),$$

   $(1, 1) = (x, x^{-1})$ as α is injective. Hence $x = 1$. Therefore $H \cap K = 1$. ■

4. Suppose $HK = G$, $H \cap K = 1$ and both H and K are normal subgroups of G. Then the mapping α in Problem 2 is an isomorphism.

   Sol. Let $h \in H$ and $k \in K$. Since both H and K are normal,

   $$K \ni (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H.$$

   Hence $hkh^{-1}k^{-1} = 1$ as $H \cap K = 1$. Therefore $hk = kh$ for all $h \in H$ and $k \in K$. Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

   $$\alpha((h_1, k_1)(h_2, k_2)) = \alpha((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \alpha((h_1, k_1))\alpha((h_2, k_2)).$$

   Hence α is a group homomorphism. Suppose $\alpha((h_1, k_1)) = \alpha((h_2, k_2))$. Then $h_1k_1 = h_2k_2$. Hence $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = 1$. Therefore $h_1 = h_2$ and $k_1 = k_2$ in this case and α is injective. Since $G = HK$, α is surjective and α is an isormorphism as desired. ■

Quiz 8

Due: 10:00 a.m. June 13, 2007

Division: **ID#:** **Name:**

Let G be a group and $\alpha : G \times G \to G$ ($(g, x) \mapsto gxg^{-1}$).

1. Show that α defines a left action of G on itself.

2. For $x \in G$, show that $\mathrm{St}_G(x) = \{g \mid (g \in G) \wedge (\alpha(g, x) = x)\}$ is a subgroup of G.

3. For $g \in G$, let $\mathrm{Fix}(g) = \{x \mid (x \in G) \wedge (\alpha(g, x) = x)\}$. Show that $\mathrm{Fix}(g) = \mathrm{St}_G(g)$, where $\mathrm{St}_G(g)$ is the subgroup defined in the previous problem.

4. Show that the kernel of this action is $Z(G) = \{x \in G \mid xg = gx \text{ (for all } g \in G)\}$.

5. Let C be the equivalence class containing x defined in Quiz 6. Show that $|G : \mathrm{St}_G(x)| = |C|$.

Message: Any questions or requests?

Solutions to Quiz 8

June 13, 2007

Let G be a group and $\alpha : G \times G \to G$ $((g, x) \mapsto gxg^{-1})$.

1. Show that α defines a left action of G on itself.

   Sol. Let $g \cdot x = \alpha(g, x) = gxg^{-1}$. Then
   $$g_1 \cdot (g_2 \cdot x) = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2)x(g_1 g_2)^{-1} = (g_1 g_2) \cdot x.$$
   Moreover $1 \cdot x = 1x1^{-1} = x$. Hence α defines a left action of G on itself. ∎

   Note that $G \times G \to G$ $(x \mapsto gx)$ also defines a left action. But clearly the above α defines a different left action.

2. For $x \in G$, show that $\mathrm{St}_G(x) = \{g \mid (g \in G) \wedge (\alpha(g, x) = x)\}$ is a subgroup of G.

   Sol. $\mathrm{St}_G(x) = \{g \mid (g \in G) \wedge (\alpha(g, x) = x)\}$ is always a subgroup for all left actions. Let $g_1, g_2 \in \mathrm{St}_G(x)$. Then $\alpha(g_1, x) = x$ and $\alpha(g_2, x) = x$. Firstly since $\alpha(1, x) = x$, $1 \in \mathrm{St}_G(x)$. Secondly since
   $$\alpha(g_1 g_2, x) = \alpha(g_1, \alpha(g_2, x)) = \alpha(g_1, x) = x,$$
   $g_1 g_2 \in \mathrm{St}_G(x)$. Thirdly
   $$\alpha(g_1^{-1}, x) = \alpha(g_1^{-1}, \alpha(g_1, x)) = \alpha(g_1^{-1} g_1, x) = \alpha(1, x) = x.$$
   Hence $g_1^{-1} \in \mathrm{St}_G(x)$ and $\mathrm{St}_G(x)$ is a subgroup of G, which is called the stabilizer of x. ∎

3. For $g \in G$, let $\mathrm{Fix}(g) = \{x \mid (x \in G) \wedge (\alpha(g, x) = x)\}$. Show that $\mathrm{Fix}(g) = \mathrm{St}_G(g)$, where $\mathrm{St}_G(g)$ is the subgroup defined in the previous problem.

   Sol. Since $\mathrm{St}_G(g)$ is a subgroup of G,
   $$\begin{aligned}\mathrm{Fix}(g) &= \{x \mid (x \in G) \wedge (\alpha(g, x) = x)\} = \{x \in G \mid gxg^{-1} = x\} \\ &= \{x \in G \mid x^{-1} g x = g\} = \{y \in G \mid ygy^{-1} = g\}^{-1} = \mathrm{St}_G(g)^{-1} \\ &= \mathrm{St}_G(g). \quad ∎\end{aligned}$$

4. Show that the kernel of this action is $Z(G) = \{x \in G \mid xg = gx \text{ (for all } g \in G)\}$.

   Sol. Let K be the kernel of this action. Then
   $$\begin{aligned}K &= \{g \in G \mid \alpha(g, x) = x \text{ for all } x \in G\} = \{g \in G \mid gxg^{-1} = x \text{ for all } x \in G\} \\ &= \{g \in G \mid gx = xg \text{ for all } x \in G\} = Z(G). \quad ∎\end{aligned}$$

5. Let C be the equivalence class containing x defined in Quiz 6. Show that $|G : \mathrm{St}_G(x)| = |C|$.

   Sol. This follows from a general theorem (5.2.1) in the textbook. But we give a proof here in this particular case. Let $H = \mathrm{St}_G(x)$.
   $$\alpha(g_1, x) = \alpha(g_2, x) \Leftrightarrow g_1 x g_1^{-1} = g_2 x g_2^{-1} \Leftrightarrow g_2^{-1} g_1 x (g_2^{-1} g_1)^{-1} = x \Leftrightarrow g_2^{-1} g_1 \in H.$$
   Hence $\alpha(g_1, x) = \alpha(g_2, x) \Leftrightarrow g_1 H = g_2 H$. Since
   $$C = \{gxg^{-1} \mid g \in G\} = \{\alpha(g, x) \mid g \in G\},$$
   $|C| = |G : H|$ as desired. ∎