Quiz 1

Due: 10:00 a.m. April 19, 2006

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

Let m be a positive integer. Let $[a] = \{a + mq \mid q \in \boldsymbol{Z}\}$ denote the congruence class modulo m containing a, and $\boldsymbol{Z}_m = \{[a] \mid a \in \boldsymbol{Z}\}$.

1. Show that the sum defined by $[a] + [b] = [a + b]$ is *well-defined*, i.e., if $[a] = [a']$ and $[b] = [b']$ for $a, a', b, b' \in \boldsymbol{Z}$, then $[a + b] = [a' + b']$.

2. Show that the product defined by $[a] \cdot [b] = [a \cdot b]$ is *well-defined*, i.e., if $[a] = [a']$ and $[b] = [b']$ for $a, a', b, b' \in \boldsymbol{Z}$, then $[a \cdot b] = [a' \cdot b']$.

3. Let $m = 14$. Find all elements $[a] \in \boldsymbol{Z}_{14}$ such that there exists $x \in \boldsymbol{Z}_{14}$ satisfying $[a][x] = [1]$.

4. Let $[a]^6 = [a][a][a][a][a][a]$ in $\boldsymbol{Z}_{14}$. Show that if $\gcd\{a, 14\} = 1$, then $[a]^6 = [1]$.

5. Let a be an integer such that $\gcd\{a, 14\} = 1$. Show that $14 \mid (a^6 - 1)$.

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

Solutions to Quiz 1

April 15, 2006

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

Let m be a positive integer. Let $[a] = \{a + mq \mid q \in \boldsymbol{Z}\}$ denote the congruence class modulo m containing a, and $\boldsymbol{Z}_m = \{[a] \mid a \in \boldsymbol{Z}\}$.

1. Show that the sum defined by $[a] + [b] = [a + b]$ is *well-defined*, i.e., if $[a] = [a']$ and $[b] = [b']$ for $a, a', b, b' \in \boldsymbol{Z}$, then $[a + b] = [a' + b']$.

   Sol. Observe that $[c] = [c']$ if and only if $m \mid (c - c')$. (See p.24.) So if $[a] = [a']$ and $[b] = [b']$, $m \mid (a - a')$ and $m \mid (b - b')$. Thus $m \mid (a - a') + (b - b') = (a + b) - (a' + b')$. Thus $[a + b] = [a' + b']$. ■

   In mathematics the term "well-defined" is often used. In this particular case, well-definedness stands for $[a] + [b] = [a + b]$ actually defines a binary operation, that is if $[a]$ and $[b]$ are given $[a + b]$ is uniquely determined regardless of expressions of $[a]$ and $[b]$. Note that there are many expressions of elements $[a]$ and $[b]$ as $[a] = [a + mp]$ and $[b] = [b + mq]$ for any integers p and q. What we showed above is that regardless of the expressions $[a + b]$ or $[a + mp + b + mq]$ gives the same member in $\boldsymbol{Z}_m$. Therefore we can carry out computations in $\boldsymbol{Z}_m$ freely using this definition.

2. Show that the product defined by $[a] \cdot [b] = [a \cdot b]$ is *well-defined*, i.e., if $[a] = [a']$ and $[b] = [b']$ for $a, a', b, b' \in \boldsymbol{Z}$, then $[a \cdot b] = [a' \cdot b']$.

   Sol. Suppose $[a] = [a']$ and $[b] = [b']$. Then $m \mid (a - a')$ and $m \mid (b - b')$. Therefore

   $$m \mid (a - a')b + a'(b - b') = ab - a'b + a'b - a'b' = ab - a'b'.$$

   Thus $[ab] = [a'b']$. ■

3. Let $m = 14$. Find all elements $[a] \in \boldsymbol{Z}_{14}$ such that there exists $x \in \boldsymbol{Z}_{14}$ satisfying $[a][x] = [1]$.

   Sol. Let $d = \gcd\{a, 14\}$. If $[1] = [a][x] = [ax]$ then there exists $q \in \boldsymbol{Z}$ such that $ax = 1 + 14q$. Since $d \mid (ax - 14q) = 1$, $d = 1$. Hence $[x] \in \{[1], [3], [5], [9], [11], [13]\}$. Observe that

   $$[1][1] = [1],\ [3][5] = [5][3] = [1],\ [9][11] = [-3][-5] = [1],\ [13][13] = [-1][-1] = [1].$$

   Hence all elements in the set $U = \{[1], [3], [5], [9], [11], [13]\}$ have the property. ■

   See (2.3.5) and (2.3.6). U is often written as $\boldsymbol{Z}_{14}^*$. (See p.41.)

4. Let $[a]^6 = [a][a][a][a][a][a]$ in $\boldsymbol{Z}_{14}$. Show that if $\gcd\{a, 14\} = 1$, then $[a]^6 = [1]$.

   Sol. $[3]^2 = [3][3] = [9]$, $[3]^3 = [9][3] = [-5][3] = [-15] = [-1] = [13]$, $[3]^4 = [-1][3] = [-3] = [11]$, $[3]^5 = [-3][3] = [-9] = [5]$, $[3]^6 = [1]$. Since every element of U above is written as a power of $[3]$, say $[a] = [3]^i$, $[a]^6 = ([3]^i)^6 = ([3]^6)^i = [1]$. ■

   We can also use (2.3.4). Since 7 is a prime, we have $7 \mid (a^7 - a) = a(a^6 - 1)$. Since a is relatively prime to 14, it is relatively prime to 7. Hence by (2.2.5) $7 \mid (a^6 - 1)$. Since a is odd and $a^6 - 1$ is even, $14 \mid (a^6 - 1)$. This implies $[a]^6 = [1]$.

5. Let a be an integer such that $\gcd\{a, 14\} = 1$. Show that $14 \mid (a^6 - 1)$.

   Sol. Since $[1] = [a]^6 = [a^6]$. $14 \mid (a^6 - 1)$. ■

Quiz 2

Due: 10:00 a.m. April 26, 2006

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

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

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

2. Express each of σ and $\pi\sigma\pi^{-1}$ as a product of disjoint cycles.

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

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

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

Message: Any questions, comments or requests?

Solutions to Quiz 2

April 26, 2006

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

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

   Sol.

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

2. Express each of σ and $\pi\sigma\pi^{-1}$ as a product of disjoint cycles.

   Sol.

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

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

   Sol.

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

   Use the formula in Corollary 3.1.4.

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

   Sol.

$$\begin{aligned}
\pi &= (2,3)(1,2)(2,3)(1,2)(5,6)(4,5)(3,4)(2,3)(1,2)(2,3)(3,4)(4,5)(5,6)(4,5)(3,4) \\
&\quad (2,3)(1,2)(2,3)(3,4)(4,5)(3,4)(2,3)(1,2)(2,3)(3,4) \\
&= (3.4)(2,3)(3,4)(4,5)(5,6)(1,2)(2,3)\ \textit{Shortest!} \\
\sigma &= (7,8)(6,7)((5,6)(4,5)(3,4)(2,3)(1,2)(7,8)(4,5)(3,4)(2,3)(5,6)(4,5)(3,4) \\
&\quad (6,7)(5,6)(4,5)(5,6)\ \textit{Shortest!}
\end{aligned}$$

   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 $\ell(\pi) = 7$, $\mathrm{sign}(\pi) = (-1)^7 = -1$. Similarly since $\ell(\sigma) = (-1)^{18}$, $\mathrm{sign}(\pi) = (-1)^{18} = 1$. Since π is the product of 3 cycles, $\mathrm{sign}(\pi) = (-1)^{8-3} = -1$ 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 8, 2006

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

1. Let S be the subset of $\boldsymbol{Z}_{14} = \{[a] \mid a \in \boldsymbol{Z}\} = \{[0], [1], \ldots, [13]\}$ ($[a] = [a]_{14} = \{a + 14q \mid q \in \boldsymbol{Z}\}$) specified below and define $[a] \cdot [b] = [a \cdot b]$. Say in each case whether $(S, \cdot)$ is a semigroup, a monoid, a group, or none of these.

   (a) $S = \{[1], [3], [5], [7], [9], [11], [13]\}$;

   (b) $S = \{[1], [3], [5], [9], [11], [13]\}$;

   (c) $S = \{[2], [4], [8]\}$;

   (d) $S = \{[0], [2], [4], [6], [8], [10], [12]\}$.

2. Let $(M, \circ)$ be a semigroup with the following two conditions: (i) There exists an element e such that for every $x \in M$, $x \circ e = x$. (ii) For each element $x \in M$ there exists $x' \in M$ such that $x \circ x' = e$.

   (a) Show that e is an identity element, i.e., $x \circ e = x = e \circ x$ for every $x \in M$. (Hint: Let $x', x'' \in M$ such that $x \circ x' = e = x' \circ x''$, which are guaranteed to exist by (ii). Compute $x \circ x' \circ x \circ x' \circ x''$ in two ways to show $e \circ x = x$.)

   (b) Show that $(M, \circ)$ is a group.

3. Define a binary operation $*$ on a set $S = \{a, b\}$ so that $(S, *)$ is a semigroup satisfying the following conditions (i) and (ii') but not a monoid: (i) There exists an element e such that for every $x \in S$, $x * e = x$. (ii') For each element $x \in S$ there exists $x' \in S$ such that $x' * x = e$.

Message: Any requests or questions?

Solutions to Quiz 3

April 29, 2006

1. Let S be the subset of $\boldsymbol{Z}_{14} = \{[a] \mid a \in \boldsymbol{Z}\} = \{[0], [1], \ldots, [13]\}$ ($[a] = [a]_{14} = \{a + 14q \mid q \in \boldsymbol{Z}\}$) specified below and define $[a] \cdot [b] = [a \cdot b]$. Say in each case whether $(S, \cdot)$ is a semigroup, a monoid, a group, or none of these.

   Since all of these subsets are closed under multiplication and $(\boldsymbol{Z}_{14}, \cdot)$ is a semigroup (and a monoid with $[1]$ as its inverse), these are either a semigroup, a monoid or a group.

   (a) $S = \{[1], [3], [5], [7], [9], [11], [13]\}$;
   Sol. *A monoid with* $[1]$ *as its identity element.* $[7]$ does not have its inverse. ■

   (b) $S = \{[1], [3], [5], [9], [11], [13]\}$;
   Sol. *A group with* $[1]$ *as its identity element, and* $[1]^{-1} = [1], [3]^{-1} = [5], [5]^{-1} = [3], [9]^{-1} = [11], [11]^{-1} = [9], [13]^{-1} = [13]$. This group is denoted by $\boldsymbol{Z}_{14}^*$. See p.41 (iv). ■

   (c) $S = \{[2], [4], [8]\}$;
   Sol. *A group with* $[8]$ *as its identity element.* ■

   (d) $S = \{[0], [2], [4], [6], [8], [10], [12]\}$.
   Sol. *A semigroup.* ■

2. Let $(M, \circ)$ be a semigroup with the following two conditions: (i) There exists an element e such that for every $x \in M$, $x \circ e = x$. (ii) For each element $x \in M$ there exists $x' \in M$ such that $x \circ x' = e$.

   (a) Show that e is an identity element, i.e., $x \circ e = x = e \circ x$ for every $x \in M$. (Hint: Let $x', x'' \in M$ such that $x \circ x' = e = x' \circ x''$, which are guaranteed to exist by (ii). Compute $x \circ x' \circ x \circ x' \circ x''$ in two ways to show $e \circ x = x$.)
   Sol. It suffices to show that $e \circ x = x$ for every $x \in M$. Let $x \in M$. Then by the condition (ii), there exists $x' \in M$ such that $x \circ x' = e$. Since $x' \in M$, there exists $x'' \in M$ such that $x' \circ x'' = e$ by (ii). Now we have $e \circ x = x$ by the following.

$$\begin{aligned} e \circ x &= (e \circ x) \circ e = ((x \circ x') \circ x) \circ (x' \circ x'') = x \circ ((x' \circ (x \circ x')) \circ x'') \\ &= x \circ ((x' \circ e) \circ x'') = x \circ (x' \circ x'') = x' \circ e = x. \end{aligned}$$

   (b) Show that $(M, \circ)$ is a group.
   Sol. It is enough to show that $x = x''$ if $x \circ x' = e = x' \circ x''$. First by (a), $e \circ x'' = x''$. Hence $x'' = e \circ x'' = x \circ x' \circ x'' = x \circ e = x$.

3. Define a binary operation $*$ on a set $S = \{a, b\}$ so that $(S, *)$ is a semigroup satisfying the following conditions (i) and (ii') but not a monoid: (i) There exists an element e such that for every $x \in S$, $x * e = x$. (ii') For each element $x \in S$ there exists $x' \in S$ such that $x' * x = e$.

   Sol. Let $a = e$ and $e * e = e, b * e = b$, $e * b = e$ and $b * b = b$. Then this operation gives the left most element in the product. Hence $(S, *)$ is a semigroup, and satisfies both (i) and (ii'), but neither $e = a$ nor b is an identity element. ■

Quiz 4

Due: 10:00 a.m. May 15, 2006

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

1. Find all subgroups of $(\boldsymbol{Z}_6, +)$. $([a] + [b] = [a + b]$ for all $a, b \in \boldsymbol{Z}$.)

2. Find all subgroups of $(\boldsymbol{Z}_9^*, \cdot)$ ($\boldsymbol{Z}_9^*$ is the set of invertible elements in a monoid $\boldsymbol{Z}_9$ with respect to the multiplication $[a] \cdot [b] = [ab]$.)

3. Show that $(\boldsymbol{Z}_9^*, \cdot)$ is a cyclic group.

4. Find all elements of the subgroup of S_3 generated by the set $\{(1, 2), (1, 2, 3)\}$.

5. Show that S_3 is not a cyclic group.

Message: Any questions or requests?

Solutions to Quiz 4

May 8, 2006

1. Find all subgroups of $(\boldsymbol{Z}_6, +)$. ($[a] + [b] = [a + b]$ for all $a, b \in \boldsymbol{Z}$.)

   Sol. $\boldsymbol{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. Let H be a subgroup of $\boldsymbol{Z}_6$. If H contains $[1]$, then H contains $[2] = [1] + [1]$, $[3] = [2] + [1]$, $[4] = [3] + 1$, $[5] = [4] + [1]$ and $[0] = [5] + [1]$. Hence $H = \boldsymbol{Z}_6$. If H contains $[5]$, then it must contain $-[5] = [1]$. Hence $H = \boldsymbol{Z}_6$. Suppose H contains neither $[1]$ nor $[5]$. If H contains either $[2]$ or $[4]$, $H = \langle [2] \rangle = \{[0], [2], [4]\}$ as $-[2] = [4]$ because if H further contains $[3]$, it contains $[5] = [2] + [3]$, a contradiction. If H does not contain $[1], [2], [4], [5]$, then $H = \{[0]\}$ or $H = \langle [3] \rangle = \{[0], [3]\}$. Hence the following are the subgroups of $\boldsymbol{Z}_6$.

   $$\{[0]\},\ \{[0], [3]\},\ \{[0], [2], [4]\},\ \text{and } \boldsymbol{Z}_6.$$

2. Find all subgroups of $(\boldsymbol{Z}_9^*, \cdot)$ ($\boldsymbol{Z}_9^*$ is the set of invertible elements in a monoid $\boldsymbol{Z}_9$ with respect to the multiplication $[a] \cdot [b] = [ab]$.)

   Sol. $\boldsymbol{Z}_9^* = \{[1], [2], [4], [5], [7], [8]\}$. Let H be a subgroup of $\boldsymbol{Z}_9^*$. Since $\langle [2] \rangle = \langle [5] \rangle = \boldsymbol{Z}_9^*$, if H contains either $[2]$ or $[5]$, $H = \boldsymbol{Z}_9^*$. Suppose H contains neither $[2]$ nor $[5]$. Since $\langle [4] \rangle = \langle [7] \rangle = \{[1], [4], [7]\}$ and if this subgroup further contain $[8]$, then it must contain $[4][8] = [5]$. Hence we can conclude that the following are the subgroups of $\boldsymbol{Z}_9^*$.

   $$\{[1]\},\ \{[1], [8]\},\ \{[1], [4], [7]\},\ \text{and } \boldsymbol{Z}_9^*.$$

3. Show that $(\boldsymbol{Z}_9^*, \cdot)$ is a cyclic group.

   Sol. Since $\boldsymbol{Z}_9^* = \langle [2] \rangle$, $\boldsymbol{Z}_9^*$ is a cyclic group. ■

   Actually, $\boldsymbol{Z}_9^*$ is isomorphic to $\boldsymbol{Z}_6$ by the following correspondence:

   $$\alpha([1]) = [0], \alpha([2]) = [1], \alpha([4]) = \alpha([2]^2) = [1] + [1] = [2], \ldots, \alpha([2]^m) = [m].$$

   Please check that α is a bijection satisfying $\alpha(a \cdot b) = \alpha(a) + \alpha(b)$.

4. Find all elements of the subgroup of S_3 generated by the set $\{(1, 2), (1, 2, 3)\}$.

   Sol. $(1, 2)(1, 2, 3) = (2, 3)$, $(1, 2, 3)(1, 2) = (1, 3)$, $(1, 2, 3)(1, 2, 3) = (1, 3, 2)$, and $(1, 2)(1, 2) = id$. Hence all elements of S_3 are in $\langle (1, 2), (1, 2, 3) \rangle$. ■

   The identity element can be recognized as a product of zero elements of the set $\{(1, 2), (1, 2, 3)\}$. As for product, all elements are multiplied to the identity element.

5. Show that S_3 is not a cyclic group.

   Sol. $(1, 2)^2 = (1, 3)^2 = (2, 3)^2 = id$ and $(1, 2, 3)^3 = (1, 3, 2)^3 = id$. Hence there is no element of order 6. ■

   Since cyclic groups are commutative (why?) S_3 cannot be cyclic as it is not commutative as indicated by the computation in the previous problem.

Quiz 5

Due: 10:00 a.m. May 22, 2006

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

1. Let H be a subgroup of a gourp G.

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

   (b) For $x, y \in G$, show that $xH = yH \Leftrightarrow Hx^{-1} = Hy^{-1}$.

   (c) Let G/H be the set of left cosets of H in G, and let $H\backslash G$ be the set of right cosets of H in G. Then the mapping $\phi : G/H \to H\backslash G$ $(xH \mapsto Hx^{-1})$ is a bijection.

2. Let $G = S_3$ be the symmetric group of degree three. Let $H = \langle(1, 2)\rangle$. Determine G/H and $H\backslash G$ and the correspondence between them in the previous problem.

Message: Any questions or requests?

Solutions to Quiz 5

May 22, 2006

1. Let H be a subgroup of a gourp G.

   First we prove the following: (i) $HH = H$, (ii) $H^{-1} = H$.

   Proof. Since H is a subgroup of G, $HH \subset H$ and $H^{-1} \subset H$. Since $1 \in H$, $H = H1 \subset HH$. Hence $HH = H$. Since $H = \{(h^{-1})^{-1} \mid h \in H\} \subset H^{-1} \subset H$, $H = H^{-1}$. ■

   (a) For $x, y \in G$, show that $xH = yH \Leftrightarrow x^{-1}y \in H$.
   Sol. Suppose $xH = yH$. Since H is a subgroup of G, $1 \in H$. Hence
   $$x^{-1}y \in x^{-1}y1 \in x^{-1}yH = x^{-1}xH = 1H = H.$$
   Conversely suppose $x^{-1}y \in H$. Then
   $$xH = xHH \supset xx^{-1}yH = yH = yHH \supset y(x^{-1}y)^{-1}H = yy^{-1}xH = xH.$$
   Hence $xH = yH$. ■

   (b) For $x, y \in G$, show that $xH = yH \Leftrightarrow Hx^{-1} = Hy^{-1}$.
   Sol. Suppose $xH = yH$. Then $(xH)^{-1} = (yH)^{-1}$. So
   $$Hx^{-1} = H^{-1}x^{-1} = (xH)^{-1} = (yH)^{-1} = H^{-1}y^{-1} = Hy^{-1}.$$
   Conversely suppose $Hx^{-1} = Hy^{-1}$. Then
   $$xH = xH^{-1} = (Hx^{-1})^{-1} = (Hy^{-1})^{-1} = yH^{-1} = yH. \quad ■$$

   (c) Let G/H be the set of left cosets of H in G, and let $H\backslash G$ be the set of right cosets of H in G. Then the mapping $\phi : G/H \to H\backslash G$ $(xH \mapsto Hx^{-1})$ is a bijection.
   Sol. First the mapping is defined by $xH \mapsto (xH)^{-1}$. Since $(xH)^{-1} = H^{-1}x^{-1} = Hx^{-1}$, $(xH)^{-1} \in H\backslash G$. Now ϕ is injective because $Hx^{-1} = \phi(xH) = \phi(yH) = Hy^{-1}$ implies $xH = yH$ by the previous problem. ϕ is surjective because $\phi(x^{-1}H) = Hx$ for every $Hx \in H\backslash G$. ■
   Let $P(G)$ denote the set of subsets of G. Then the mapping $\psi : P(G) \to P(G)$ $(A \mapsto A^{-1})$ is a bijection as $\psi \circ \psi = id_{P(X)}$. Moreover, $\psi(G/H) \subset H\backslash G$ as $\phi(xH) = Hx^{-1}$. Since ϕ is defined by $\psi_{|G/H}$, ϕ is injective.

2. Let $G = S_3$ be the symmetric group of degree three. Let $H = \langle(1,2)\rangle$. Determine G/H and $H\backslash G$ and the correspondence between them in the previous problem.

   Sol. $G = S_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$ and $H = \{1, (1,2)\}$. Since $|H| = 2$ and $|G| = 6$, $|G : H| = 3$. $G/H = \{H, (1,2,3)H, (1,3,2)H\}$ as $(1,2,3) \notin H$, $(1,3,2) \notin H$ and $(1,2,3)^{-1}(1,3,2) = (1,3,2)(1,3,2) = (1,2,3) \notin H$. Moreover, $(1,2,3)H = \{(1,2,3), (1,3)\}$ and $(1,3,2)H = \{(1,3,2), (2,3)\}$. Now $H(1,2,3)^{-1} = H(1,3,2) = \{(1,3,2), (1,3)\}$ and $H(1,3,2)^{-1} = \{(1,3,2), (2,3)\}$.

   Therefore $H\backslash G = \{H, H(1,3,2), H(1,2,3)\}$ and $\phi(H) = H$, $\phi((1,2,3)H) = H(1,3,2)$ and $\phi((1,3,2)H) = H(1,2,3)$. ■

   In this particular case, by setting $K = \langle(1,2,3)\rangle = \{1, (1,2,3), (1,3,2)\}$, $G = KH = HK$ and K is a left transversal and a right transversal of H in G.

Quiz 6

Due: 10:00 a.m. May 31, 2006

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

1. Let N be a subgroup of a group G. Show the following.
$$xNx^{-1} \subseteq N \text{ for all } x \in G \Rightarrow xN = Nx \text{ for all } x \in G.$$

2. Let $\sigma \in S_n$. Show that $\sigma(i_1, i_2, i_3, \ldots, i_m)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \sigma(i_3), \ldots, \sigma(i_m))$, where $(i_1, i_2, i_3, \ldots, i_m)$ is an m-cycle.

3. Show that if a normal subgroup N of S_n contains an m-cycle for some $2 \leq m \leq n$, then N contains all m-cycles.

4. Determine all normal subgroups of S_3.

5. Determine all normal subgropus of S_4.

Message: Any questions or requests?

Solutions to Quiz 6

May 31, 2006

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

$$xNx^{-1} \subseteq N \text{ for all } x \in G \Rightarrow xN = Nx \text{ for all } x \in G.$$

Sol. By multiplying x from the right we have $xN \subseteq Nx$ for all $x \in G$. Since $xNx^{-1} \subseteq N$ holds for all $x \in G$, it holds for x^{-1}. Hence $x^{-1}N(x^{-1})^{-1} \subseteq N$. By multiplying x from the left we have $Nx \subseteq xN$. Since x is arbitrary, we have $xN = Nx$ for all $x \in G$. ■

Let $\ell_x : G \to G$ $(g \mapsto xg)$. Then ℓ_x is a bijection. Note that multiplying x from the left to the sets $x^{-1}Nx$ and N is to map these sets by ℓ_x. So $Nx = \ell_x(x^{-1}Nx) \subseteq \ell(N) = xN$, or take $x^{-1}nx \in x^{-1}Nx$ and map it by ℓ_x.

2. Let $\sigma \in S_n$. Show that $\sigma(i_1, i_2, i_3, \ldots, i_m)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \sigma(i_3), \ldots, \sigma(i_m))$, where $(i_1, i_2, i_3, \ldots, i_m)$ is an m-cycle.

Sol. $\sigma(i_1, i_2, i_3, \ldots, i_m)\sigma^{-1}(\sigma(i_j)) = \sigma(i_1, i_2, i_3, \ldots, i_m)(i_j) = \sigma(i_{i+1})$ or $\sigma(i_1)$ if $j = m$. If $j \notin \{i_1, i_2, \ldots, i_m\}$, $\sigma(i_1, i_2, i_3, \ldots, i_m)\sigma^{-1}(\sigma(j)) = \sigma(i_1, i_2, i_3, \ldots, i_m)(j) = \sigma(j)$. Therefore $\sigma(i_1, i_2, i_3, \ldots, i_m)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \sigma(i_3), \ldots, \sigma(i_m))$. ■

3. Show that if a normal subgroup N of S_n contains an m-cycle for some $2 \leq m \leq n$, then N contains all m-cycles.

Sol. Suppose N contains an m-cycle $(i_1, i_2, \ldots, i_m)$. Let $(j_1, j_2, \ldots, j_m)$ be an arbitrary m-cycle. Let

$$\{1, 2, \ldots, n\} = \{i_1, i_2, \ldots, i_m, i_{m+1}, \ldots, i_n\} = \{j_1, j_2, \ldots, j_m, j_{m+1}, \ldots, j_n\}$$

and let $\sigma(i_s) = j_s$ for all s. Then by the previous problem, $\sigma(i_1, i_2, \ldots, i_m)\sigma^{-1} = (j_1, j_2, \ldots, j_m)$ and this element belongs to N. So all m-cycles are contained in N. ■

4. Determine all normal subgroups of S_3.

Sol. Let N be a normal subgroup of S_3. N contains 1. If N contains a transposition, i.e., a 2-cycle, then N contains all three transpositions by the previous problem. Then N contains at least four elements. Since $|N|$ divides $|S_3| = 6$, we have $N = S_3$. Since $A_3 = \{1, (1, 2, 3), (1, 3, 2)\}$ is a normal subgroup of G, N is either 1, A_3 or S_3. ■

5. Determine all normal subgropus of S_4.

Sol. S_4 consists of the identity element, 6 transpositions, 8 three cycles, and 6 four cycles and three elements of type $(i_1, i_2)(i_3, i_4)$. Let N be a normal subgroup of G. Then $|N|$ divides 24 and is a sum of 1 and some of $6, 8, 6, 3$. The only possibilities are 1, $1 + 3$, $1 + 3 + 8$, $1 + 3 + 6 + 8 + 6$. Thus $N = 1$, $V = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$, A_4 or S_4. It is easy to check that V is also a normal subgroup and it is called the Klein's Four Group. Note that in the problem 3, the case of a product of two transpositions is not dealt, but the proof includes such case. ■

Quiz 7

Due: 10:00 a.m. June 7, 2006

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

1. Let $\alpha : G \to H$ be a group homomorphism. Let N be a normal subgroup of H, and $\alpha^{-1}(N) = \{x \in G \mid \alpha(x) \in N\}$.

   (a) Show that $\alpha^{-1}(N)$ is a subgroup of G.

   (b) Show that $\alpha^{-1}(N)$ is a normal subgroup of G.

2. Let H and K be groups, and $G = H \times K$. Show that $H \times K$ becomes a group by the following binary operation. For $(h_1, k_1), (h_2, k_2) \in H \times K$, $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$.

3. Let $\alpha : \boldsymbol{Z} \to \boldsymbol{Z}_3 \times \boldsymbol{Z}_5 \quad (n \mapsto ([n]_3, [n]_5))$, where $[n]_3$ is the equivalence class containing n modulo 3, and $[n]_5$ is the equivalence class containing n modulo 5.

   (a) Show that α is a surjective homomorphism.

   (b) Show that $\mathrm{Ker}(\alpha) = 15\boldsymbol{Z} = \{n \in \boldsymbol{Z} \mid 15 \mid n\}$ and that $\boldsymbol{Z}_3 \times \boldsymbol{Z}_5$ is a cyclic group.

Message: Any questions or requests?

Solutions to Quiz 7

June 7, 2006

1. Let $\alpha : G \to H$ be a group homomorphism. Let N be a normal subgroup of H, and $\alpha^{-1}(N) = \{x \in G \mid \alpha(x) \in N\}$.

   (a) Show that $\alpha^{-1}(N)$ is a subgroup of G.
   Sol. Let $K = \alpha^{-1}(N)$. Since $\alpha(1_G) = 1_H \in N$, $1_G \in K$. Let $x, y \in K$. Then $\alpha(x), \alpha(y) \in N$. Since N is a subgroup of H, $\alpha(xy) = \alpha(x)\alpha(y) \in N$ and $\alpha(x^{-1}) = \alpha(x)^{-1} \in N$. Therefore $xy \in K$ and $x^{-1} \in K$ and K is a subgroup of G. ■
   (I used the fact that if α is a homomorphism, $\alpha(xy) = \alpha(x)\alpha(t)$, $\alpha(1) = 1$ and $\alpha(x^{-1}) = \alpha(x)^{-1}$. Then (3.3.3) is applied.)

   (b) Show that $\alpha^{-1}(N)$ is a normal subgroup of G.
   Sol. Let $g \in G$ and $x \in K = \alpha^{-1}(N)$. By (4.2.1) it suffices to show that $gxg^{-1} \in K$. Since N is a normal subgroup of G, $\alpha(gxg^{-1}) = \alpha(g)\alpha(x)\alpha(g)^{-1} \in \alpha(g)N\alpha(g)^{-1} \subset N$. Hence $gxg^{-1} \in K$. ■

2. Let H and K be groups, and $G = H \times K$. 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. ■

3. Let $\alpha : \boldsymbol{Z} \to \boldsymbol{Z}_3 \times \boldsymbol{Z}_5$ $(n \mapsto ([n]_3, [n]_5))$, where $[n]_3$ is the equivalence class containing n modulo 3, and $[n]_5$ is the equivalence class containing n modulo 5.

   (a) Show that α is a surjective homomorphism.
   Sol. First α is a homomorphism because
   $$\begin{aligned} \alpha(m+n) &= ([m+n]_3, [m+n]_5) = ([m]_3 + [n]_3, [m]_5 + [n]_5) \\ &= ([m]_3, [m]_5) + ([n]_3, [n]_5) = \alpha(m) + \alpha(n). \end{aligned}$$
   We show that there is $n \in \boldsymbol{Z}$ such that $\alpha(n) = ([a]_3, [b]_5)$ for all $a, b \in \boldsymbol{Z}$. Since 3 and 5 are relatively prime, there exist $x, y \in \boldsymbol{Z}$ such that $3x + 5y = 1$. Thus let $n = 3bx + 5ay$. Then
   $$\begin{aligned} \alpha(n) &= ([3bx + 5ay]_3, [3bx + 5ay]_5) = ([5ay]_3, [3bx]_5) \\ &= ([a(1-3x)]_3, [b(1-5y)]_5) = ([a]_3, [b]_5). \end{aligned}$$
   Therefore α is a surjective homomorphism. (See (2.3.7).) ■

   (b) Show that $\mathrm{Ker}(\alpha) = 15\boldsymbol{Z} = \{n \in \boldsymbol{Z} \mid 15 \mid n\}$ and that $\boldsymbol{Z}_3 \times \boldsymbol{Z}_5$ is cyclic.
   Sol. Since $\alpha(15m) = ([15m]_3, [15m]_5) = ([0]_3, [0]_5)$, $15\boldsymbol{Z} \subseteq \mathrm{Ker}(\alpha)$. If $n \in \mathrm{Ker}(\alpha)$, then $[n]_3 = [0]_3$ and $[n]_5 = [0]_5$. Hence $3 \mid n$ and $5 \mid n$. Let $x, y \in \boldsymbol{Z}$ such that $3x + 5y = 1$. Then $n = 3xn + 5yn$. Since $3 \mid n$ and $5 \mid n$, both $3xn$ and $5yn$ are divisible by 15. Hence n is divisible by 15, and $n \in 15\boldsymbol{Z}$. Since $\boldsymbol{Z}/15\boldsymbol{Z} \simeq \boldsymbol{Z}_3 \times \boldsymbol{Z}_5$ and $\boldsymbol{Z}/15\boldsymbol{Z}$ is cyclic, $\boldsymbol{Z}_3 \times \boldsymbol{Z}_5$ is cyclic as well. ■

Quiz 8

Due: 10:00 a.m. June 14, 2006

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

Let G be a group, H a subgroup and $\alpha : G \times G/H \to G/H$ $((g, xH) \mapsto gxH)$.

1. Show that α defines a left action of G on the set G/H.

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

3. Show that $\mathrm{St}_G(xH) = xHx^{-1}$, where $\mathrm{St}_G(xH)$ is the subgroup defined above.

4. Suppose $|G : H| = 3$. Let $N = \mathrm{Ker}(G, G/H)$. Show that $|G : N| = 3$ or 6.

5. Suppose $G = S_3$ and $H = \{1, (1, 2)\}$. Determine $\mathrm{Ker}(G, G/H)$ in this case.

Message: Any questions or requests?

Solutions to Quiz 8

June 14, 2006

Let G be a group, H a subgroup and $\alpha : G \times G/H \to G/H$ ($(g, xH) \mapsto gxH$).

1. Show that α defines a left action of G on the set G/H.

   Sol. Let $\alpha(g, xH) = g \cdot xH$. (i) $g_2 \cdot (g_1 \cdot xH) = g_2 g_1 xH = (g_2 g_1) \cdot xH$ and (i) holds. $1_G \cdot xH = 1xH = xH$ and (ii) holds. Hence α defines a left action of G on the set G/H. ■

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

   Sol. Since $1_G \cdot xH = xH$, $1_G \in \mathrm{St}_G(xH)$. Let $g_1, g_2 \in \mathrm{St}_G(xH)$. Then $(g_1 g_2) \cdot xH = g_1 \cdot (g_2 \cdot xH) = g_1 \cdot xH = xH$. Hence $g_1 g_2 \in \mathrm{St}_G(xH)$. Since $g_1^{-1} \cdot xH = g_1^{-1} \cdot (g_1 \cdot xH) = 1_G \cdot xH = xH$, $g_1^{-1} \in \mathrm{St}_G(xH)$. Hence $\mathrm{St}_G(xH) \leq G$. ■

3. Show that $\mathrm{St}_G(xH) = xHx^{-1}$, where $\mathrm{St}_G(xH)$ is the subgroup defined above.

   Sol. Let $g \in \mathrm{St}_G(xH)$. Then $gxH = xH$. Hence $g \in gx1x^{-1} \in gxHx^{-1} = xHx^{-1}$ and $\mathrm{St}_G(xH) \subseteq xHx^{-1}$. On the other hand if $g \in xHx^{-1}$, there exists $h \in H$ such that $g = xhx^{-1}$. Now $gxH = xhx^{-1}xH = xhH = xH$. So $xHx^{-1} \subseteq \mathrm{St}_G(xH)$. Note that $aH = bH$ if and only if $a^{-1}b \in H$, and hence we have $H = hH$ if and only if $h \in H$. ■

   In particular $xHx^{-1} \leq G$.

4. Suppose $|G : H| = 3$. Let $N = \mathrm{Ker}(G, G/H)$. Show that $|G : N| = 3$ or 6.

   Sol. Since $|G/H| = 3$, there is a homomorphism $\hat{\alpha} : G \to \mathrm{Sym}(G/H) \simeq S_3$. Hence by the isomorphism theorem, G/N is isomorphic to a subgroup of S_3. Since $N \leq H$, $|G : N| = |G : H||H : N| = 3|H : N|$. Thus we have the result. ■

   We used the fact that $|S_3| = 6$ and $N = \bigcap_{x \in G} xHx^{-1} \subseteq H$.

5. Suppose $G = S_3$ and $H = \{1, (1, 2)\}$. Determine $\mathrm{Ker}(G, G/H)$ in this case.

   Sol. Since $(1, 3)H(1, 3) \neq H$, $N < H$. Hence $|G : N| = 6$, and $N = \mathrm{Ker}(G, G/H) = 1$. ■