Quiz 1

Due: 10:10 a.m. April 21, 2008

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

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

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

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

Solutions to Quiz 1

April 21, 2008

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

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

   Sol.

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

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.

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

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

   Sol.

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

   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 $(1,2), (2,3), \ldots, (7,8)$. (Is it a shortest?)

   Sol.

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

   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 $\ell(\sigma) = (-1)^{13}$, $\mathrm{sign}(\pi) = (-1)^{13} = -1$. 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 3 cycles, $\mathrm{sign}(\sigma) = (-1)^{8-3} = -1$.

Quiz 2

Due: 10:10 a.m. April 28, 2008

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

1. Let $\boldsymbol{R}$ be the set of real numbers, and $G = \boldsymbol{R} \setminus \{-1\} = \{x \mid (x \in \boldsymbol{R}) \wedge (x \neq -1)\}$. For $x, y \in G$, let $x * y = xy + x + y$. Show that $(G, *)$ is a group. Do not forget to check that $*$ defines a binary operation on G.

2. Let $(G, \circ)$ is a group with the identity element e. Suppose that $x \circ x = e$ for all $x \in G$. Show that $(G, \circ)$ is an abelian group, i.e., $x \circ y = y \circ x$ for all $x, y \in G$.

Message: Any questions, comments or requests?

Solutions to Quiz 2

April 28, 2008

1. Let $\boldsymbol{R}$ be the set of real numbers, and $G = \boldsymbol{R} \setminus \{-1\} = \{x \mid (x \in \boldsymbol{R}) \wedge (x \neq -1)\}$. For $x, y \in G$, let $x * y = xy + x + y$. Show that $(G, *)$ is a group. Do not forget to check that $*$ defines a binary operation on G.

   Sol. Note that $x * y = (x+1)(y+1) - 1$.

   Clearly $x * y \in \boldsymbol{R}$. Suppose $-1 = x * y = (x+1)(y+1) - 1$. Then $(x+1)(y+1) = 0$. Since $x \neq -1$ and $y \neq -1$, this is absurd. Hence $x * y \in G$ for all $x, y \in G$.

   Let $x, y, z \in G$. Then

   $$(x*y)*z = ((x+1)(y+1)-1)*z = (x+1)(y+1)(z+1)-1 = x*((y+1)(z+1)-1) = x*(y*z).$$

   Since $x * 0 = (x+1) - 1 = x = 0 * x$, 0 plays as the identity element in G. Let $x \in G$. Then

   $$x * \left(\frac{1}{x+1} - 1\right) = (x+1)\frac{1}{x+1} - 1 = 0 = \frac{1}{x+1}(x+1) - 1 = \left(\frac{1}{x+1} - 1\right) * x.$$

   Hence x has its inverse. Note that as $x \neq -1$, $\frac{1}{x+1} - 1 \in G$. Therefore $(G, *)$ is a group. ■

2. Let $(G, \circ)$ is a group with the identity element e. Suppose that $x \circ x = e$ for all $x \in G$. Show that $(G, \circ)$ is an abelian group, i.e., $x \circ y = y \circ x$ for all $x, y \in G$.

   Sol. By applications of the general associativity law, we omit parentheses. Let $x, y \in G$. Since $x \circ y \in G$, $x \circ y \circ x \circ y = e$, and $x \circ x = y \circ y = e$. Hence

   $$y \circ x = y \circ x \circ e = y \circ x \circ x \circ y \circ x \circ y = y \circ e \circ y \circ x \circ y = y \circ y \circ x \circ y = e \circ x \circ y = x \circ y.$$

   Therefore, $(G, \circ)$ is an abelian group. ■

Quiz 3

Due: 10:10 a.m. May 7, 2008

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

Let $\boldsymbol{Z}_{18} = \{[0], [1], \ldots, [17]\}$ be a group with addition as its binary operation, and $\boldsymbol{Z}_{18}^*$ be a group with multiplication as its binary operation. Recall that $\boldsymbol{Z}_{18}^*$ is the set of invertible elements in $\boldsymbol{Z}_{18}$ with respect to multiplication.

1. Find all elements in $\langle [3] \rangle$, i.e., the subgroup generated by $[3]$, and the order of $[3]$ in $\boldsymbol{Z}_{18}$.

2. Find all elements $[a] \in \boldsymbol{Z}_{18}$ such that $\langle [3] \rangle = \langle [a] \rangle$.

3. Find all elements in $\boldsymbol{Z}_{18}^*$.

4. Show that $[a]^6 = [1]$ for all $[a] \in \boldsymbol{Z}_{18}^*$.

5. Determine whether or not $\boldsymbol{Z}_{18}^*$ is a cyclic group.

Message: Any requests or questions?

Solutions to Quiz 3

May 7, 2008

Let $\boldsymbol{Z}_{18} = \{[0], [1], \dots, [17]\}$ be a group with addition as its binary operation, and $\boldsymbol{Z}_{18}^*$ be a group with multiplication as its binary operation. Recall that $\boldsymbol{Z}_{18}^*$ is the set of invertible elements in $\boldsymbol{Z}_{18}$ with respect to multiplication.

1. Find all elements in $\langle [3] \rangle$, i.e., the subgroup generated by [3], and the order of [3] in $\boldsymbol{Z}_{18}$.

   Sol. Since $[3]+[3] = [6]$, $[3]+[3]+[3] = [6]+[3] = [9]$, $[3]+[3]+[3]+[3] = [12]$ and $[3]+[3]+[3]+[3]+[3]+[3] = [0]$, we have the following by Proposition 3.4 (3.3.6).
   $$\langle [3] \rangle = \{[0], [3], [6], [9], [12], [15]\}$$
   and hence the order of [3], denoted by $|[3]| = |\langle [3] \rangle| = 6$.

   (Note that when the operation is addition, we customarily denote $[3]+[3] = 2[3]$, $[3]+[3]+[3] = 3[3]$ instead of using power notation.) ■

2. Find all elements $[a] \in \boldsymbol{Z}_{18}$ such that $\langle [3] \rangle = \langle [a] \rangle$.

   Sol. If the condition is satisfied, $[a] \in \langle [3] \rangle = \{[0], [3], [6], [9], [12], [15]\}$. Check one by one we find $[a] = [3]$, or $[15]$.

   (Note that if $[a] = m[3]$, then the greatest common divisor of m and 6 has to be 1 and we have $m = 1$ or 5 if $0 \le m \le 5$. See (4.1.7), (4.1.8).) ■

3. Find all elements in $\boldsymbol{Z}_{18}^*$.

   Sol. If $[a][b] = [ab] = [1]$ in $\boldsymbol{Z}_{18}$, there exists an integer m such that $ab - 1 = 18m$. Hence $ab - 18m = 1$. If d is a common divisor of a and 18, then it must divide 1. Hence if $[a]$ is invertible in $\boldsymbol{Z}_{18}$ with respect to multiplication, a is coprime to 18. Conversely if a is coprime to 18, there are integers x and y satisfying $ax + 18y = 1$. Then $[a][x] = [ax] = [1 - 18y] = [1]$ and $[a]$ is invertible. Therefore
   $$\boldsymbol{Z}_{18}^* = \{[1], [5], [7], [11], [13], [17]\}.$$
   Therefore $|\boldsymbol{Z}_{18}^*| = 6$. ■

4. Show that $[a]^6 = [1]$ for all $[a] \in \boldsymbol{Z}_{18}^*$.

   Sol. $[5]^2 = [5][5] = [25] = [7]$, $[5]^3 = [5][5][5] = [7][5] = [35] = [17] = [-1]$, $[5]^4 = [5][5][5][5] = [-1][5] = [-5] = [13]$, $[5]^5 = [5][5][5][5][5] = [-7] = [11]$, $[5]^6 = [5][5][5][5][5][5] = [1]$. Hence all elements of $\boldsymbol{Z}^*18$ appear as a power of [5] and $[5]^6 = [1]$. Thus $[a] = [5]^i$ for some i and $[a]^6 = ([5]^i)^6 = ([5]^6)^i = [1]$. This proves the assertion. ■

5. Determine whether or not $\boldsymbol{Z}_{18}^*$ is a cyclic group.

   Sol. By the previous problem, we have shown that
   $$\boldsymbol{Z}_{18}^* = \{[5]^n \mid n \in \boldsymbol{Z}\} = \langle [5] \rangle.$$
   Thus $\boldsymbol{Z}_{18}^*$ is a cyclic group. ■

Quiz 4

Due: 10:10 a.m. May 14, 2008

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

1. Let G be a group and H a nonempty subset of G. Show that if $H^{-1}H \subseteq H$, then $H \leq G$.

2. Let H be a subgroup of a group G, and $a, b \in G$. Show the following.

   (a) $H = H^{-1}$.

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

   (c) If $a^{-1}b \in H$, then $aH = bH$.

   (d) If $aH = bH$, then $a^{-1}b \in H$.

Message: Any questions or requests?

Solutions to Quiz 4

May 14, 2008

1. Let G be a group and H a nonempty subset of G. Show that if $H^{-1}H \subseteq H$, then $H \leq G$.

   Sol. (Since H is nonempty, it suffices to show that $xy \in H$ and $x^{-1} \in H$ for all $x, y \in H$.)

   Since H is nonempty, there is an element $x \in H$. Hence $1 = x^{-1}x \in H^{-1}H \subseteq H$. Thus $x^{-1} = x^{-1}1 \in H^{-1}H \subseteq H$. Let $x, y \in H$. Since $x^{-1} \in H$, $xy = (x^{-1})^{-1}y \in H^{-1}H \subseteq H$. Therefore $xy \in H$ and $x^{-1} \in H$ for all $x, y \in H$. ■

2. Let H be a subgroup of a group G, and $a, b \in G$. Show the following.

   (a) $H = H^{-1}$.

   Sol. Since H is a subgroup, $H^{-1} \subseteq H$. Let $h \in H$. Since H is a subgroup of G, $h^{-1} \in H$. Therefore $h = (h^{-1})^{-1} \in H^{-1}$ and $H \subseteq H^{-1}$. Thus $H = H^{-1}$. ■

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

   Sol. Let $x, y \in H$. Since H is a subgroup of G, $x^{-1} \in H$ and $x^{-1}y \in H$. Hence $H^{-1}H \subseteq H$. Since H is a subgroup of G, $1 \in H$. Therefore $h = 1^{-1}h \in H^{-1}H$ and $H \subseteq H^{-1}H$. Thus $H^{-1}H = H$. ■

   (c) If $a^{-1}b \in H$, then $aH = bH$.

   Sol.

   $$aH = bb^{-1}aH = b(a^{-1}b)^{-1}H \subseteq bH^{-1}H = bH \subseteq aa^{-1}bH \subseteq aHH \subseteq aH.$$

   Hence $aH = bH$. ■

   (d) If $aH = bH$, then $a^{-1}b \in H$.

   Sol.

   $$a^{-1}b = a^{-1}b1 \in a^{-1}bH = a^{-1}aH = H.$$

   Therefore $a^{-1}b \in H$. ■

Quiz 5

Due: 10:10 a.m. May 21, 2008

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

Let $G = S_4$, the symmetric group of degree 4, $V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, $K = \{1, (1,2)(3,4)\}$, and $H = \langle (1,2), (1,3) \rangle$. Show the following.

1. $K \lhd V$, i.e., K is a normal subgroup of V.

2. $V \lhd G$, i.e., V is a normal subgroup of G.

3. K is not a normal subgroup of G.

4. G/V is not an abelian group.

5. $G = VH$ and $V \cap H = 1$.

Message: Any questions or requests?

Solutions to Quiz 5

May 21, 2008

Let $G = S_4$, the symmetric group of degree 4, $V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, $K = \{1, (1,2)(3,4)\}$, and $H = \langle (1,2), (1,3) \rangle$. Show the following.

1. $K \lhd V$, i.e., K is a normal subgroup of V.

   Sol. Let $\sigma \in V$. Then clearly $\sigma^2 = 1$. $\sigma^{-1} = \sigma$.

$$\begin{aligned}(1,2)(3,4)(1,3)(2,4) &= (1,4)(2,3) = (1,3)(2,4)(1,2)(3,4),\\ (1,2)(3,4)(1,4)(2,3) &= (1,3)(2,4) = (1,4)(2,3)(1,2)(3,4),\\ (1,3)(2,4)(1,4)(2,3) &= (1,2)(3,4) = (1,4)(2,3)(1,3)(2,4).\end{aligned}$$

   Hence $V \leq G$, and V is abelian. Since $K = \langle (1,2)(3,4) \rangle$, K is a subgroup of V. Since V is abelian, K is a normal subgroup of V. ■

2. $V \lhd G$, i.e., V is a normal subgroup of G.

   Sol. First note that V contains all permutations of type $(a,b)(c,d)$ in S_4. Let $\sigma \in S_4$. Then
$$\sigma(a,b)(c,d)\sigma^{-1} = (\sigma(a), \sigma(b))(\sigma(c), \sigma(d)).$$
   Hence $\sigma\pi\sigma^{-1} \in V$ for all $1 \neq \pi \in V$. It is clear that $\sigma 1 \sigma^{-1} = 1 \in V$, and V is a normal subgroup of G. ■

3. K is not a normal subgroup of G.

   Sol. Since $(1,3)(1,2)(3,4)(1,3) = (2,3)(1,4) \not\in K$, K is not normal in G. ■

4. G/V is not an abelian group.

   Sol. $(1,2)(2,3)(1,2)(2,3) = (1,2,3)(1,2,3) = (1,3,2) \not\in V$. Hence $G' \not\leq V$ and G/V is not abelian.

   By our computation above,
$$((1,2)V)((2,3)V)((1,2)V)^{-1}((2,3)V)^{-1} = (1,3,2)V \neq V$$
   Hence $((1,2)V)((2,3)V) \neq ((2,3)V)((1,2)V)$. ■

5. $G = VH$ and $V \cap H = 1$.

   Sol. Since $H = \{1, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}$, $V \cap H = 1$ part is clear. Since
$$|VH| = |V||H|/|V \cap H| = 24 = |G|.$$
   Therefore $VH = G$.

   Let $x, y \in H$. If $Vx = Vy$, then $yx^{-1} \in V \cap H = 1$. Hence distinct elements in H belong to distinct cosets in G/V. Hence $|VH| = |V||H| = 24$. Therefore $G = VH$ as $VH \subseteq G$. ■

Quiz 6

Due: 10:00 a.m. May 28, 2008

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

Let m and n be positive integers. Let π be an assignment from $\boldsymbol{Z}_n$ to $\boldsymbol{Z}_m$ defined by $[a]_n \mapsto [a]_m$.

1. Show that if π is a mapping from $\boldsymbol{Z}_n$ to $\boldsymbol{Z}_m$, then $m \mid n$, i.e., there exists $\ell \in \boldsymbol{Z}$ such that $n = \ell m$.

2. Suppose $\ell \mid n$ and $m \mid n$. Then a mapping $\alpha : \boldsymbol{Z}_n \to \boldsymbol{Z}_\ell \times \boldsymbol{Z}_m$ ($[a]_n \mapsto ([a]_\ell, [a]_m)$) is a homomorphism.

3. Show that the mapping α above is injective if and only if the least common multiple of ℓ and m is n.

4. Show that the mapping α above is surjective if and only if the greatest common divisor of ℓ and m is 1.

5. Show that if $n = \ell m$, and ℓ and m are coprime integers., i.e., $\gcd(\ell, m) = 1$, then $\boldsymbol{Z}_n \simeq \boldsymbol{Z}_\ell \times \boldsymbol{Z}_m$.

Message: Any questions or requests?

Solutions to Quiz 6

May 28, 2008

Let m and n be positive integers. Let π be an assignment from $\boldsymbol{Z}_n$ to $\boldsymbol{Z}_m$ defined by $[a]_n \mapsto [a]_m$.

1. Show that if π is a mapping from $\boldsymbol{Z}_n$ to $\boldsymbol{Z}_m$, then $m \mid n$, i.e., there exists $\ell \in \boldsymbol{Z}$ such that $n = \ell m$.

   Sol. Suppose π is a mapping. Since $[n]_n = [0]_n$, $[n]_m = [0]_m$. Hence $m \mid n$.

   Conversely suppose $m \mid n$. If $[a]_n = [b]_n$, then $n \mid a - b$. Since $m \mid n$, $m \mid a - b$ and $[a]_m = [b]_m$. Therefore π is a well-defined mapping. ■

2. Suppose $\ell \mid n$ and $m \mid n$. Then a mapping $\alpha : \boldsymbol{Z}_n \to \boldsymbol{Z}_\ell \times \boldsymbol{Z}_m$ ($[a]_n \mapsto ([a]_\ell, [a]_m)$ is a homomorphism.

   Sol. By 1, the assignments $[a]_n \mapsto [a]_\ell$ and $[a]_n \mapsto [a]_m$ are mappings. Hence α is a well-defined mapping. Now

   $$\begin{aligned} \alpha([a]_n + [b]_n) &= \alpha([a+b]_n) = ([a+b]_\ell, [a+b]_m) = ([a]_\ell + [b]_\ell, [a]_m + [b]_m) \\ &= ([a]_\ell, [a]_m) + ([b]_\ell, [b]_m) = \alpha([a]_n) + \alpha([b]_n). \end{aligned}$$

   Hence α is a homomorphism. ■

3. Show that the mapping α above is injective if and only if the least common multiple of ℓ and m is n.

   Sol. Suppose α is injective. Then $\alpha([a]_n) = ([a]_\ell, [a]_m) = ([0]_\ell, [0]_m)$ implies $[a]_n = [0]$. Hence $m \mid a$ and $\ell \mid a$ implies $n \mid a$. By assumption n is a common multiple of ℓ and m. Let a be a common multiple of ℓ and m. Then clearly $\ell \mid a$ and $m \mid a$. Hence $n \mid a$. Thus n is the least common multiple of ℓ and m.

   Suppose n is the least common multiple of ℓ and m. If a is a common multiple of ℓ and m, then $n \mid a$. Hence we have $\alpha([a]_n) = ([a]_\ell, [a]_m) = ([0]_\ell, [0]_m)$ implies $[a]_n = [0]_n$, and α is injective. ■

4. Show that the mapping α above is surjective if and only if the greatest common divisor of ℓ and m is 1.

   Sol. Suppose α is surjective. Then there exists $[a]_n$ such that $[a]_\ell = [1]_\ell$ and $[a]_m = [0]_m$. Hence there are integers s and t such that $a = ms = \ell t + 1$. Hence $ms - \ell t = 1$. If d is the greatest common divisor of ℓ and m, then d divides $ms - \ell t = 1$. Hence $d = 1$.

   Conversely if ℓ and m are coprime each other, there are integers s and t such that $s\ell + tm = 1$. (To prove this fact consider $\langle \ell, m \rangle$ in $\boldsymbol{Z}$. Since $\boldsymbol{Z}$ is cyclic and every subgroup of a cyclic group is cyclic, there exists a nonnegative integer d such that $\langle \ell, m \rangle = \langle d \rangle$. Since $\ell, m \in \langle \ell, m \rangle$, $d \mid \ell$ and $d \mid m$. Hence $d = 1$. Since $d \in \langle \ell, m \rangle$, there exist integers s, t such that $1 = s\ell + tm$.) Now let x and y are arbitrary integers. Then $[xtm + ys\ell]_\ell = [xtm]_\ell = [x(1 - s\ell)]_\ell = [x]_\ell$, and $[xtm + ys\ell]_m = [ys\ell]_m = [y(1 - tm)]_m = [y]_m$ and α is surjective. ■

5. Show that if $n = \ell m$, and ℓ and m are coprime integers., i.e., $\gcd(\ell, m) = 1$, then $\boldsymbol{Z}_n \simeq \boldsymbol{Z}_\ell \times \boldsymbol{Z}_m$.

   Sol. By 3 and 4, the mapping α above is an isomorphism. Hence we have $\boldsymbol{Z}_n \simeq \boldsymbol{Z}_\ell \times \boldsymbol{Z}_m$. ■

Quiz 7

Due: 10:10 a.m. June 4, 2008

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

Let G be a finite group of order p^n, where p is a prime number, and X a non-empty finite set. Let $\alpha : G \times X \to X$ $((g, x) \mapsto g \cdot x)$ be a left action of G on X. For $x, y \in X$ we write $x \sim y$ if there is an element $g \in G$ such that $y = g \cdot x$. Let $C_X(G) = \{x \in X \mid g \cdot x = x \text{ for all } g \in G\}$.

1. Show that the relation $\sim$ on X is an equivalence relation.

2. For $x \in X$ let $[x]$ denote the equivalence class with respect to $\sim$ containing x. (This is called an *orbit* and denoted by $G \cdot x$.) Show that $x \in C_X(G) \Leftrightarrow |[x]| = 1$.

3. Show that $|[x]|$ is a power of p for all $x \in X$. (Hint: (5.2.1) or Proposition 7.3 in the lecture.)

4. Show that $|X| \equiv |C_X(G)| \pmod{p}$.

Message: Any questions or requests?

Solutions to Quiz 7

June 4, 2008

Let G be a finite group of order p^n, where p is a prime number, and X a non-empty finite set. Let $\alpha : G \times X \to X$ ($(g, x) \mapsto g \cdot x$) be a left action of G on X. For $x, y \in X$ we write $x \sim y$ if there is an element $g \in G$ such that $y = g \cdot x$. Let $C_X(G) = \{x \in X \mid g \cdot x = x \text{ for all } g \in G\}$.

Since α is a left action, it satisfies; (i) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $g_1, g_2 \in G$ and $x \in X$, (ii) $1 \cdot x = x$ for all $x \in X$, where 1 denotes the identity element of G.

1. Show that the relation $\sim$ on X is an equivalence relation.

   Sol. Since $1 \cdot x = x$ by (i), $x \sim x$. If $x \sim y$, there exists $g \in G$ such that $g \cdot x = y$. Now $g^{-1} \in G$ and

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

   Hence $y \sim x$. Suppose $x \sim y$ and $y \sim z$. Then there exists $g_1, g_2 \in G$ such that $g_1 \cdot x = y$ and $g_2 \cdot y = z$. Then by (ii), $(g_2 g_1) \cdot x = g_2 \cdot (g_1 \cdot x) = g_2 \cdot y = z$. Since $g_2 g_1 \in G$, $x \sim z$. Hence $\sim$ is an equivalence relation. ■

2. For $x \in X$ let $[x]$ denote the equivalence class with respect to $\sim$ containing x. (This is called an *orbit* and denoted by $G \cdot x$.) Show that $x \in C_X(G) \Leftrightarrow |[x]| = 1$.

   Sol. Suppose $x \in C_X(G)$. Then $g \cdot x = x$ for all $g \in G$. Hence $[x] = \{x\}$. Conversely if $|[x]| = 1$, then $[x] = \{x\}$ as $x \in [x]$. For all $g \in G$, $x \sim g \cdot x$. Since $g \cdot x \in [x] = \{x\}$, $g \cdot x = x$ and $x \in C_X(G)$. ■

3. Show that $|[x]|$ is a power of p for all $x \in X$. (Hint: (5.2.1) or Proposition 7.3 in the lecture.)

   Sol. By (5.2.1), $|[x]| = (G : \mathrm{St}_G(x))$, where $\mathrm{St}_G(x) = \{g \in G \mid g \cdot x = x\}$. Since $\mathrm{St}_G(x) \le G$, $(G : \mathrm{St}_G(x))$ divides $|G| = p^n$. Therefore $|[x]|$ is a power of p. ■

4. Show that $|X| \equiv |C_X(G)| \pmod{p}$.

   Sol. Let $[x_1]$, $[x_2]$, $\ldots [x_m]$ be distinct equivalence classes. By the previous problem, $|[x_i]|$ is a power of p and by 2, $|[x_i]| = 1$ if and only if $x_i \in C_X(G)$. Thus $x_i \notin C_X(G)$ if and only if $|[x_i]|$ is divisible by p. Suppose $|[x_1]| = \cdots |[x_s]| = 1 < |[x_{s+1}]|, \ldots, |[x_m]|$. Then

   $$\begin{aligned} |X| &= |[x_1]| + \cdots + |[x_s]| + |[x_{s+1}]| + \cdots + |[x_m]| \\ &\equiv |[x_1]| + \cdots + |[x_s]| \pmod{p} \\ &\equiv s \pmod{p} \\ &\equiv |C_X(G)| \pmod{p}. \end{aligned}$$

   This proves the assertion. ■

Quiz 8

Due: 10:10 a.m. June 11, 2008

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

Let G be a finite group of order p^2q, where p and q are primes. Let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups and $\mathrm{Syl}_q(G)$ Sylow q-subgroups, and $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$.

1. Show that $|\mathrm{Syl}_q(G)|$ is either 1, p or p^2.

2. Suppose $|\mathrm{Syl}_q(G)| = p^2$. Then $P \lhd G$. [Hint: Show first that each Sylow q-subgroup contains $q-1$ elements of order q and there are $p^2(q-1)$ elements of order q. Show next that there are only p^2 elements of order a power of p to conclude that $P \lhd G$.]

3. Suppose $|\mathrm{Syl}_q(G)| = p$. Show that $p > q$ and $P \lhd G$.

4. Suppose $|\mathrm{Syl}_q(G)| = p$ and $H = N_G(Q)$. Let R be a Sylow p-subgroup of H. Show that $R = Z(G)$. [Hint: Using the fact that $p > q$, show that $H \simeq R \times Q$. Use the fact that each Sylow p-subgroup is abelian.]

5. Show that G is not simple.

Message: Any questions or requests?

Solutions to Quiz 8

June 11, 2008

Let G be a finite group of order p^2q, where p and q are primes. Let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups and $\mathrm{Syl}_q(G)$ Sylow q-subgroups, and $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$.

1. Show that $|\mathrm{Syl}_q(G)|$ is either 1, p or p^2.

   Sol. Let $\alpha : G \times \mathrm{Syl}_q(G) \to \mathrm{Syl}_q(G)\,(Q \mapsto gQg^{-1})$ be a left action. Then all Sylow q-subgroups are in one orbit by (5.3.8) and the length of the orbit $\mathrm{Syl}_q(G)$ of Q is $|G : \mathrm{St}_G(Q)|$. Moreover

   $$\mathrm{St}_G(Q) = \{g \in G \mid g \cdot Q = Q\} = \{g \in G \mid gQg^{-1} = Q\} = N_G(Q) \geq Q.$$

   By (4.1.3) in the textbook, $|\mathrm{Syl}_q(G)| = |G : N_G(Q)| \mid |G : Q| = p^2$. Therefore, it is either 1, p or p^2. ■

2. Suppose $|\mathrm{Syl}_q(G)| = p^2$. Then $P \lhd G$. [Hint: Show first that each Sylow q-subgroup contains $q-1$ elements of order q and there are $p^2(q-1)$ elements of order q. Show next that there are only p^2 elements of order a power of p to conclude that $P \lhd G$.]

   Sol. By assumption, $N_G(Q) = Q$. Let $x \in G - Q$. Then $Q \cap xQx^{-1} = 1$ and all elements of order q is in one of the p^2 Sylow q-subgroups. Since non identity element of each Sylow q-subgroup is of order q, there are altogether $p^2(q-1)$ element of order q. Hence $p^2q - p^2(q-1) = p^2$ is exactly the number of elements in P, $gPg^{-1} = P$ for all $g \in G$, as there are no elements of order q in gPg^{-1}. Therefore $P \lhd G$. ■

3. Suppose $|\mathrm{Syl}_q(G)| = p$. Show that $p > q$ and $P \lhd G$.

   Sol. Since $p = |\mathrm{Syl}_q(G)| \equiv 1 \pmod q$, $q \mid p-1$ and $p > q$. Now $|\mathrm{Syl}_p(G)| = |G : N_G(P)| \mid q$ and $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$, we have $|\mathrm{Syl}_p(G)| = 1$. Thus $P \lhd G$. ■

4. Suppose $|\mathrm{Syl}_q(G)| = p$ and $H = N_G(Q)$. Let R be a Sylow p-subgroup of H. Show that $R = Z(G)$. [Hint: Using the fact that $p > q$, show that $H \simeq R \times Q$. Use the fact that each Sylow p-subgroup is abelian.]

   Sol. $|H| = pq$. Hence $Q \lhd H$ and $H = RQ$. Since $|\mathrm{Syl}_p(H)| = |H : N_H(R)| \mid q$ and $|\mathrm{Syl}_p(H)| \equiv 1 \pmod p$, we have $|\mathrm{Syl}_p(H)| = 1$ as $p > q$. Thus $H \simeq R \times Q$. In particular $C_G(R) \supset Q$. Since every Sylow p-subgroup is of order p^2 and hence abelian, a Sylow subgroup containing R is contained in $C_G(R)$. Thus $|C_G(R)|$ is divisible by $p^2q = |G|$ and $C_G(R) = G$. This proves $R \subseteq Z(G)$. Since $N_G(Q) = H < G$, $p^2 \nmid |Z(G)|$ and $q \nmid |Z(G)|$, we have $Z(G) = R$. ■

5. Show that G is not simple.

   Sol. If $|\mathrm{Syl}_q(G)| = 1$, then $1 \neq Q \lhd G$. Other cases are treated above. In particular, if Q is not normal in G, then P is normal in G. ■