MATH 257: Homework #4

Jesse Farmer

27 October 2004

1. *Let $\varphi : G \to H$ be a homomorphism and $E \leq H$. Prove that $\varphi^{-1}(E) \leq G$. If $E \trianglelefteq H$ show that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that* $\ker\varphi \trianglelefteq G$.

   A subset of H of a group G is a subgroup if and only if for all $x, y \in G$, $xy^{-1} \in G$. Let $x, y \in \varphi^{-1}(E)$, then $\varphi(x), \varphi(y) \in E$. Because $E \leq H$, $\varphi(y^{-1}) = \varphi(y)^{-1} \in E$. Hence $\varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}) \in E$ and therefore $xy^{-1} \in \varphi^{-1}(E)$.

   If $E \trianglelefteq H$ and $x \in \varphi^{-1}(E)$ is arbitrary, then $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = h\varphi(x)h^{-1}$. This is in E since $\varphi(x) \in E$ and $E \trianglelefteq H$, hence $gxg^{-1} \in \varphi^{-1}(E)$ and $\varphi^{-1}(E) \trianglelefteq G$.

   $\ker\varphi = \varphi^{-1}(e)$, i.e., the kernel is the fiber of the identity element. Since $\{e\} \trianglelefteq H$, it follows that $\ker\varphi = \varphi^{-1}(\{e\}) \trianglelefteq G$.

2. *Let $\varphi : G \to H$ be a group homomorphism with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and Y the fiber above b. Fix an element u of X so $\varphi(u) = a$. Prove that if $XY = Z$ in the quotient group G/K and $w \in Z$ then there exists $v \in Y$ such that $uv = w$.*

   If $w \in XY$ then $\varphi(w) = ab$ since there exist x, y such that $w = xy$ where $\varphi(x) = a$ and $\varphi(y) = b$. If $u \in X$ is fixed any $w \in Z$ is arbitrary, then $\varphi(u^{-1}w) = \varphi(u)^{-1}\varphi(w) = a^{-1}ab = b$. Hence $u^{-1}w \in Y$, and this is precisely the v for which we are looking.

3. *Prove that if $N \trianglelefteq G$ and $H \leq G$ then $N \cap H \trianglelefteq H$.*

   Let $x \in N \cap H$. Then $x \in N$ and $x \in H$. For any $h \in H \leq G$, $hxh^{-1} \in N$ since $N \trianglelefteq G$ and $h \in G$, and $hxh^{-1} \in H$ since H is a subgroup of G. Therefore $hgh^{-1} \in N \cap H$, i.e., $N \cap H \trianglelefteq H$.

4. *Prove that if $G/Z(G)$ is cyclic then G is abelian.*

   In general, if $N \trianglelefteq G$ then $(gN)^n = g^n N$. This is easy to see through induction. Since the group operation on the quotient group is well-defined, i.e., $gHgH = HggH = g^2H$, if it is true for $n \in \mathbb{N}$ then $(gN)^{n+1} = (gN)^n gN = g^n NgN = Ng^n gN = g^{n+1}N$. That is is true for $n \in \mathbb{Z}$ is proven identically by considering $g^{-1}N$.

   Since $Z(G)$ is certainly normal – it is an abelian subgroup – this holds here. Assume $G/Z(G) =< xZ(G) >$ for some $x \in G$, then $G/Z(G) = \{(xZ(G))^n \mid n \in \mathbb{Z}\} = \{x^n Z(G) \mid n \in \mathbb{Z}\}$. If $g \in G$ then $g \in gH = x^k Z(G)$ for some $k \in \mathbb{Z}$, and hence $g = x^k z$ for some $k \in \mathbb{Z}$ and some $z \in Z(G)$. Let $g_1, g_2 \in G$ then $g_1 = x^j z$ and $g_2 = x^k z'$ for some $k, j \in \mathbb{Z}$. Since z and z' commute with every element of G,

$$g_1 g_2 = (x^j z)(x^k z') = z(x^j x^k)z' = zx^{j+k}z' = z'x^{k+j}z = z'(x^k x^j)z = (x^k z')(x^j z) = g_2 g_1$$

Therefore G is abelian

5. *Let $H \leq G$ and let $g \in G$. Show that if the right coset Hg equals some left coset of H in G then it equals gH and hence $g \in N_G(H)$.*

   Let $x \in G$ be such that $gH = Hx$, then certainly $g \in gH = Hx$. However, $g \in Hg$. Since cosets partition G, and $Hg \cap Hx \neq \emptyset$, $gH = Hx = Hg$.

6. *Prove that there are the same number of left cosets as right cosets.*

   Consider the map $\varphi(gH) = Hg^{-1}$ from the set of left cosets to the set of right cosets. The map $\varphi^{-1}(Hg) = g^{-1}H$ is both a left and right inverse since

   $$\left(\varphi \circ \varphi^{-1}\right)(Hg) = \varphi(g^{-1}H) = Hg$$

   and

   $$\left(\varphi^{-1} \circ \varphi\right)(gH) = \varphi^{-1}(Hg^{-1}) = gH$$

   Hence φ is a bijection, and so the number of left and right cosets must be equal.

7. *Let G be a finite group and $H \leq G$, $N \trianglelefteq G$. Prove that if $(|H|, [G:N]) = 1$ then $H \leq N$.*

   Let $\varphi : G \to G/N$ be the natural group homomorphism. Then $\varphi\mid_H : H \to G/N$ is still a homomorphism. This means $\ker \varphi\mid_H \trianglelefteq H$ and so $|\varphi(H)| \mid |H|$. Since $H \leq G$, $\varphi(H) \leq G/N$ and therefore $|\varphi(H)| \mid [G : N]$ by Lagrange's theorem. However, $(|H|, [G : N]) = 1$ so $|\varphi(H)| = 1$, i.e., $\varphi(H) = \{e\}$. This implies $hN = N$ for all $h \in H$ and therefore $H \leq N$.

8. *Determine the last two digits of $3^{3^{100}}$.*

   In general, the order of any element of a group divides the order of the group, and hence if $x \in |G|$ then $x^{|G|} = e$. Since an element x of the integers modulo n is a unit if and only if $(x, n) = 1$, $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ and therefore $x^{\varphi(n)} \equiv 1 \mod n$.

   Note that $\varphi(100) = 40$ and $(3, 100) = 1$, hence $3^{40} \equiv 1 \pmod{100}$. Also,

   $$3^{100} \equiv (3^4)^{10} \equiv 81^{10} \equiv 1 \pmod{40}$$

   Therefore there exists a k such that

   $$3^{3^{100}} = 3^{40k+1} \equiv 3^{40}3 \equiv 3 \pmod{100}$$

   The last two digits are 0 and 3.

9. *Let $\sigma = (1\,2\,3\,4\,5)$ in S_5. Find τ such that the following are satisfied:*

   (a) $\tau\sigma\tau^{-1} = \sigma^2$
   $\sigma^2 = (1\,3\,5\,2\,4)$, so we must find a τ such that $tau(1) = 3$, $\tau(2) = 5$, $\tau(3) = 2$, $\tau(4) = 4$, and $\tau(5) = 1$). Computing the cycles for this gives $\tau = (1\,3\,2\,5)$.

   (b) $\tau\sigma\tau^{-1} = \sigma^{-1}$
   $\sigma^{-1} = (1\,5\,4\,3\,2)$, so τ must be such that $\tau(1) = 1$, $\tau(2) = 5$, $\tau(3) = 4$, $\tau(4) = 3$, $\tau(5) = 2$. This gives $\tau = (2\,5)(3\,4)$.

   (c) $\tau\sigma\tau^{-1} = \sigma^{-2}$
   $\sigma^{-2} = (31425)$, and using the exact same procedure as the previous two yields $\tau = (1\,3\,4\,2)$.

10. *For each of the following determine if σ_1 and σ_2 are conjugate, and if so a permutation τ such that $\tau\sigma_1\tau^{-1} = \sigma_2$.*

   (a) $\sigma_1 = (1\,2)(3\,4\,5)$ *and* $\sigma_2 = (1\,2\,3)(4\,5)$.
   Yes, these two permutations are conjugate and $\tau = (1\,3\,5\,2\,4)$. The procedure used is the same as that used in the previous problems.

   (b) $\sigma_1 = (1\,5)(3\,7\,2)(10\,6\,8\,11)$ *and* $\sigma_2 = (3\,7\,5\,10)(4\,9)(13\,11\,2)$
   Yes. $\tau = (1\,4)(3\,10\,11\,7\,6\,9\,5\,8\,12\,13)$.

   (c) $\sigma_1 = (1\,5)(3\,7\,2)(10\,6\,8\,11)$ *and* $\sigma_2 = \sigma_1^3$
   These cannot be conjugate because they have different orders, 12 and 4 respectively.

   (d) $\sigma_1 = (1\,3)(2\,4\,6)$ *and* $(3\,5)(2\,4)(5\,6)$
   These cannot be conjugate either because they have different orders, 6 and 2, respectively.