Math 42001, Homework Set 5, Solutions

Problems 2.4; 13, 19, 2.5; 1, 6, 12, 14, 15, 16, 17, 27, 29, 52

November 26, 2006

p. 64, #13 Find the orders of all the elements of $U_{18}$. Is $U_{18}$ cyclic?

Solution. Notice that, $U_{18} = \{[1], [5], [7], [11], [13], [17]\}$ and

\[5^2 \equiv 7 \pmod{18}, \quad 7^2 \equiv 13 \pmod{18}, \quad 11^2 \equiv 13 \pmod{18}, \quad 13^2 \equiv 7 \pmod{18}, \quad 17^2 \equiv 1 \pmod{18} \]
\[5^3 \equiv 17 \pmod{18}, \quad 7^3 \equiv 1 \pmod{18}, \quad 11^3 \equiv 17 \pmod{18}, \quad 13^3 \equiv 1 \pmod{18} \]
\[5^4 \equiv 13 \pmod{18}, \quad 11^4 \equiv 7 \pmod{18} \]
\[5^5 \equiv 11 \pmod{18}, \quad 11^5 \equiv 5 \pmod{18} \]
\[5^6 \equiv 1 \pmod{18}, \quad 11^6 \equiv 1 \pmod{18} \]

Hence $o([1]) = 1$, $o([5]) = 6$, $o([7]) = 3$, $o([11]) = 6$, $o([13]) = 3$, $o([17]) = 2$ and so $U_{18} = ([5]) = ([11])$ is cyclic.

p. 65, #19 Find all the distinct conjugacy classes of $S_3$.

Solution. $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$

and $S_3$ has the following 3 distinct conjugacy classes:

$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$. Check it!
p. 65, #30  If in $G$ $a^5 = e$ and $aba^{-1} = b^2$, find $o(b)$ if $b \neq e$.

**Solution.** Recall that $(aba^{-1})^k = ab^ka^{-1}$ for all positive integers $k$. With this in hand, we have

$$aba^{-1} = b^2 \implies ab a^{-1} = b^{32} \implies a (b^2)^8 a^{-1} = b^{32} \implies a (aba^{-1})^8 a^{-1} = b^{32}$$

$$\implies a^2 b^8 a^{-2} = b^{32} \implies a^2 (b^2)^4 a^{-2} = b^{32} \implies a^2 (aba^{-1})^4 a^{-2} = b^{32}$$

$$\implies a^3 b^4 a^{-3} = b^{32} \implies a^3 (b^2)^2 a^{-3} = b^{32} \implies a^3 (aba^{-1})^2 a^{-3} = b^{32}$$

$$\implies a^4 b^2 a^{-4} = b^{32} \implies a^4 aba^{-1} a^{-4} = b^{32} \implies a^5 ba^{-5} = b^{32}$$

$$\implies b = b^{32} \implies e = b^{31}$$

Hence $o(b) | 31$ and since 31 is prime we have that $o(b) = 1$ or 31. As $b \neq e$ we are forced to conclude that $o(b) = 31$.

p. 73, #1 Determine in each of the parts if the given mapping is a homomorphism. If so, identify its kernel and whether or not the mapping is 1-1 or onto.

a) $G = \mathbb{Z}$ under $+$, $G' = \mathbb{Z}_n$, $\varphi(a) = [a]$ for $a \in \mathbb{Z}$.

Claim: $\varphi$ is an epimorphism, yet not a monomorphism.

Proof: Let $a, b \in G$. Notice that $\varphi(a+b) = [a+b] = [a]+[b] = \varphi(a)+\varphi(b)$. Hence $\varphi$ is a homomorphism. Now fix $1 \leq a \leq n$. Then $[a] \in G' \implies a \in G$ and $\varphi(a) = [a]$ . Hence $\varphi$ is epimorphic. Now, $\ker(\varphi) = \{a \in \mathbb{Z} | [a] = [0]\} = \{a \in \mathbb{Z} | n \mid a\} = \{nk \mid k \in \mathbb{Z}\}$. Since $\ker(\varphi) \neq (0)$, this homomorphism is not 1-1.

b) $G$ a group, $\varphi : G \rightarrow G$ defined by $\varphi(a) = a^{-1}$ for $a \in G$.

$\varphi$ is not a homomorphism in general. In fact, $\varphi$ is a homomorphism iff $G$ is abelian:

First, if $G$ is abelian and $a, b \in G$ then $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)$ and so $\varphi$ is an endomorphism.

Conversely, if $\varphi$ is an endomorphism, and $a, b \in G$ then $ab = \varphi((ab)^{-1}) = \varphi(b^{-1}a^{-1}) = \varphi(b^{-1})\varphi(a^{-1}) = ba$ fact that establishes the abelian nature of $G$. Hence if $G = S_n$ for $n \geq 3$, $\varphi$ is not a homomorphism.

c) $G$ abelian group, $\varphi : G \rightarrow G$ defined by $\varphi(a) = a^{-1}$.

Claim: $\varphi$ is an epimorphic monomorphism whose kernel is the set $\{e\}$.

We have established in part (b) that $\varphi$ is a homomorphism. Now let $a \in G$. Then $a^{-1} \in G$, and $\varphi(a^{-1}) = (\varphi(a))^{-1} = (a^{-1})^{-1} = a$. Hence $\varphi$ is epimorphic. Now, $\ker(\varphi) = \{x \in G | \varphi(x) = e\} = \{x \in G | x^{-1} = e\} = \{x \in G | x = e\} = \{e\}$ and so $\varphi$ is 1-1. Therefore $\varphi \in \text{Aut}(G)$. 

2
d) $G$ group of all nonzero real numbers under multiplication, $G' = \{-1, 1\}$, $\varphi(r) = 1$ if $r$ is positive, $\varphi(r) = -1$ if $r$ is negative.

Claim: $\varphi$ is an epimorphism whose kernel is the set $\{x \in \mathbb{R} \mid x > 0\}$.

Proof: Let $r_1, r_2 \in \mathbb{R} \setminus \{0\}$. Notice that $\varphi(r_1 r_2)$ has three cases to work out. Case I: $r_1, r_2 > 0$ in which $\varphi(r_1 r_2) = 1 = 1 \cdot 1 = \varphi(r_1) \varphi(r_2)$. Case II: Either $r_1 > 0$ and $r_2 < 0$ or $r_1 < 0$ and $r_2 > 0$. Then $\varphi(r_1 r_2) = -1 = -1 \cdot 1 = \varphi(r_1) \varphi(r_2)$. Case III: $r_1, r_2 < 0$. Then $\varphi(r_1 r_2) = 1 = 1 \cdot -1 = \varphi(r_1) \varphi(r_2)$.

Hence $\varphi$ is a homomorphism. Now, fix $x \in G'$. Then $x = -1$ or $x = 1$. If $x = 1$, then fix $r > 0$ and $\varphi(r) = 1 = x$. If $x = -1$, then fix $r < 0$ and $\varphi(r) = -1 = x$. From this it is not only clear that $\varphi$ is epimorphic, but also that $\varphi$ is NOT monomorphic, as $r$ can be any positive real number and still map to 1; $r$ can be any negative real number and still map to -1. Finally $\ker(\varphi) = \{x \in G \mid \varphi(x) = 1\} = \{x \in \mathbb{R} \mid x > 0\}$.

(This solution is entirely based on the assumption that $G'$ is taken under multiplication also.)

e) $G$ an abelian group, $n > 1$ a fixed integer, and $\varphi: G \rightarrow G$ defined by $\varphi(a) = a^n$ for $a \in G$.

Note that for $a, b \in G$ we have that $\varphi(ab) = (ab)^n = a^n b^n = \varphi(a) \varphi(b)$ thanks to the abelian nature of $G$. Hence, $\varphi$ is an endomorphism. Furthermore, $\ker(\varphi) = \{a \in G \mid a^n = e\} = \{a \in G \mid o(a) \mid n\}$.

In general, nothing further can be said about $\varphi$. If for example, the order of every element in $G$ is a divisor of $n$, then $\varphi$ is trivial. If on the other hand $(n, |G|) = 1$ then $\varphi \in \text{Aut}(G)$.

p. 74, #6 Prove that if $\varphi: G \rightarrow G'$ is a homomorphism, then $\varphi(G)$, the image of $G$, is a subgroup of $G'$.

**Proof.** First notice that $\varphi(G)$ is nonempty, as $\varphi(e) = e$. So let $a', b' \in \varphi(G)$. This implies that $\exists a, b \in G$ such that $\varphi(a) = a'$ and $\varphi(b) = b'$. Since $ab \in G$, we have $\varphi(ab) = \varphi(a) \varphi(b) = a'b' \in \varphi(G)$. Now, let $a' \in \varphi(G)$. Then $\exists a \in G$ such that $\varphi(a) = a'$. But $\varphi(a^{-1}) = (\varphi(a))^{-1} = (a')^{-1} \in \varphi(G)$. Therefore $\varphi(G)$ is a subgroup of $G'$.

p. 74, #12 Prove that if $Z(G)$ is the center of $G$, then $Z(G) \triangleleft G$.

**Proof.** First we must show that $Z(G) \leq G$. This is not difficult, since we already have $e \in Z(G)$. Now let $z_1, z_2 \in Z(G)$. Then fix $x \in G$. Notice that $xz_1z_2 = z_1xz_2 = z_1z_2x$, so $Z(G)$ has closure. Now let $z \in Z(G)$. Then $z^{-1} \in G$ clearly. Let $x \in G$, and notice that $xz^{-1} = (zx^{-1})^{-1} = (x^{-1}z)^{-1} = z^{-1}x$.

Hence $z^{-1} \in Z(G)$. So, we have established that $Z(G) \leq G$. Now we fix $z \in Z(G)$, and let $x \in G$. Notice that $x^{-1}z = z^{-1}xz = z \in Z(G)$. Hence $Z(G) \triangleleft G$.

p. 74, #14 If $G$ is abelian and $\varphi: G \rightarrow G'$ is a homomorphism of $G$ onto $G'$, prove that $G'$ is abelian.

**Proof.** Fix $a', b' \in G'$. Since $\varphi$ is onto, $\exists a, b \in G$ such that $\varphi(a) = a'$ and $\varphi(b) = b'$. Now, $a'b' = \varphi(a) \varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b) \varphi(a) = b'a'$. Therefore $G'$ is abelian.
p. 74, #15 If $G$ is any group, $N \triangleleft G$, and $\varphi : G \longrightarrow G'$ a homomorphism of $G$ onto $G'$, prove that the image, $\varphi(N)$, of $N$ is a normal subgroup of $G'$.

**Proof.** The fact that $\varphi(N) \leq G'$, is established on problem (6) since $\varphi|_{N} : N \to G'$ is a group homomorphism. To see that $\varphi(N) \triangleleft G'$, fix $a' \in \varphi(N)$ and $x' \in G'$. Since $\varphi$ is surjective, there are $x \in G$ and $a \in N$ such that $\varphi(x) = x'$ and $\varphi(a) = a'$. Since $N \triangleleft G$, we have $xax^{-1} \in N$ and so $x'ax^{-1} = \varphi(x)\varphi(a)\varphi(x^{-1}) = \varphi(xax^{-1}) \in \varphi(N)$. Therefore $\varphi(N) \triangleleft G'$. ■

p. 74, #16 If $N \triangleleft G$ and $M \triangleleft G$ and $MN = \{mn \mid m \in M, n \in N\}$, prove that $MN$ is a subgroup of $G$ and that $MN \triangleleft G$.

**Proof.** Clearly $e \in MN$ as $e \in M$ and $e \in N$ and $e = ee$. Now let $m_1, m_2 \in M$ and $n_1, n_2 \in N$. Then $(m_1n_1)(m_2n_2)^{-1} = m_1n_1n_2^{-1}m_2^{-1} = (m_1m_2^{-1})(m_2n_1^{-1}n_2^{-1}) \in MN$ since $m_1m_2^{-1} \in M, m_2 (n_1n_2^{-1}) m_2^{-1} \in N$, thanks to the normality of $N$ in $G$. Hence, $MN \leq G$. Now for $m \in M, n \in N$, and $x \in G$ we have that $xmnx^{-1} = (xmx^{-1})(nx^{-1}) \in MN$ since $N \triangleleft G$ and $M \triangleleft G$, ensures that $xmx^{-1} \in M$ and $xnx^{-1} \in N$. ■

p. 74, #17 If $M \triangleleft G, N \triangleleft G$, prove that $M \cap N \triangleleft G$.

**Proof.** First we must establish that $M \cap N \leq G$. Clearly $e \in M \cap N$ since $e \in M$ and $e \in N$. Next let $a, b \in M \cap N$. Therefore $ab \in M$, and $ab \in N$, which implies $ab \in M \cap N$. Finally, let $a \in M \cap N$. Then $a \in M, a \in N \implies a^{-1} \in M, a^{-1} \in N \implies a^{-1} \in M \cap N$. Therefore $M \cap N \leq G$. Now, fix $a \in M \cap N$ and let $x \in G$. Since $M \triangleleft G, N \triangleleft G, x^{-1}ax \in M$ and $x^{-1}ax \in N$. Therefore $x^{-1}ax \in M \cap N$, and we have that $M \cap N \triangleleft G$. ■

p. 75, #27 If $\theta$ is an automorphism of $G$ and $N \triangleleft G$, prove that $\theta(N) \triangleleft G$.

**Proof.** This is a special case of problem (15). ■
A subgroup $T$ of a group $W$ is called characteristic if $\varphi(T) \subset T$ for all automorphisms, $\varphi$, of $W$. Prove that:

a) $M$ characteristic in $G$ implies that $M \triangleleft G$.

b) $M, N$ characteristic in $G$ implies $MN$ characteristic in $G$.

c) A normal subgroup of a group need not be characteristic. (This is quite hard; you must find an example of a group $G$ and a noncharacteristic normal subgroup).

**Solution.** We establish the following small auxiliary result:

**Lemma 1** Let $G$ be a group and $g \in G$. Then the map $\alpha_g : G \to G$ defined by $\alpha_g(x) = gxg^{-1}$ is an automorphism of $G$. In fact, $\alpha_g$ is called an inner automorphism of $G$. The set of all inner automorphisms of $G$ is denoted by Inn($G$) and it is a normal subgroup of Aut($G$), the group of all automorphisms of $G$.

**Proof of lemma.** For $x, y \in G$ we have that $\alpha_g(xy) = gx(g^{-1})gy = (gx)(gy) = \alpha_g(x)\alpha_g(y)$, fact that establishes the endomorphic nature of $\alpha_g$. Furthermore, $\ker(\alpha_g) = \{x \in G \mid \alpha_g(x) = e\} = \{x \in G \mid gxg^{-1} = e\} = \{x \in G \mid gx = g\} = \{x \in G \mid x = e\} = \{e\}$ and so $\alpha_g$ is injective. Also for any $y \in G$ we have that $g^{-1}yg \in G$ and $\alpha_g(g^{-1}yg) = g^{-1}ygg^{-1} = y$, fact that makes $\alpha_g$ surjective. Hence $\alpha_g \in$ Aut($G$). We now establish the rest of the lemma even though it is not necessary for this exercise:

Note that $i_G = \alpha_e \in$ Inn($G$). Furthermore for $g, h, x \in G$, we have that $(\alpha_g \circ \alpha_{g^{-1}})(x) = \alpha_g(\alpha_{g^{-1}}(x)) = \alpha_g(g^{-1}x) = g^{-1}xgg^{-1} = x$ and $(\alpha_{g^{-1}} \circ \alpha_g)(x) = \alpha_{g^{-1}}(\alpha_g(x)) = \alpha_{g^{-1}}(gxg^{-1}) = g^{-1}gg^{-1}x = x$ and so $\alpha_g \circ \alpha_{g^{-1}} = \alpha_{g^{-1}} \circ \alpha_g = i_G$. Hence $\alpha_g^{-1} = \alpha_{g^{-1}} \in$ Inn($G$). Also $(\alpha_g \circ \alpha_h)(x) = \alpha_g(\alpha_h(x)) = \alpha_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \alpha_{gh}(x)$. It follows then that $\alpha_g \circ \alpha_h = \alpha_{gh} \in$ Inn($G$). Thus so far we have established that Inn($G$) $\leq$ Aut($G$). It remains to show that Inn($G$) $\triangleleft$ Aut($G$). So fix $g, x \in G$ and $f \in$ Aut($G$). Then $(f \circ \alpha_g \circ f^{-1})(x) = f(\alpha_g(f^{-1}(x))) = f(gf^{-1}(x)g^{-1}) = f(g) f((f^{-1}(x)) f(g^{-1}) = [f(g)]x[f(g)]^{-1} = \alpha_{f(g)}(x)$. Thus $f \circ \alpha_g \circ f^{-1} = \alpha_{f(g)} \in$ Inn($G$) and the normality is established. $\blacksquare$

a) Let $x \in G$. By the lemma $\alpha_x \in$ Aut($G$) and since $M$ is characteristic in $G$, we have that $xMx^{-1} = \alpha_x(M) \subset M$. Thus $M \triangleleft G$.

b) From problem (16) and part (a) we know that $MN \triangleleft G$. In order to see that $MN$ is characteristic in $G$, let $\varphi \in$ Aut($G$), $m \in M$, and $n \in N$. As both $M, N$ are characteristic in $G$, we conclude that $\varphi(m) \in M$ and $\varphi(n) \in N$ forcing $\varphi(mn) = \varphi(m)\varphi(n) \in MN$. Thus, $\varphi(MN) \subset MN$ and so $MN$ is characteristic in $G$. 


c) Consider the group $\mathbb{R}$ of real numbers under addition and its subgroup $\mathbb{Z}$ of integers. Since $\mathbb{R}$ is abelian then all its subgroups, and in particular $\mathbb{Z}$, are normal. Now it is easy to see that the map $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \frac{x}{2}$ is an automorphism of $\mathbb{R}$. On the other hand $f(\mathbb{Z}) \not\subseteq \mathbb{Z}$ since $f(1) = \frac{1}{2} \not\in \mathbb{Z}$.

p. 77, #52 Let $G$ be a finite group and $\varphi$ an automorphism of $G$ such that $\varphi(x) = x^{-1}$ for more than three-fourths of the elements of $G$. Prove that $\varphi(y) = y^{-1}$ for all $y \in G$, and so $G$ is abelian.

**Proof.** Define $S = \{ x \in G \mid \varphi(x) = x^{-1} \}$ and fix $g \in S$. Define $Sg^{-1} = \{ xg^{-1} \in G \mid x \in S \}$. Observe that the map $\lambda : S \to Sg^{-1}$ defined by $\lambda(x) = xg^{-1}$ for all $x \in S$ is injective, for if $\lambda(x_1) = \lambda(x_2)$ for some $x_1, x_2 \in S$ then $x_1g^{-1} = x_2g^{-1}$ and so $x_1 = x_2$ by cancellation. Hence $|Sg^{-1}| \geq |S| \geq \frac{3}{4} |G|$. Therefore $|G| \geq |S \cup Sg^{-1}| = |S| + |Sg^{-1}| - |S \cap Sg^{-1}| > \frac{3}{4} |G| + \frac{3}{4} |G| - |S \cap Sg^{-1}| = \frac{3}{2} |G| - |S \cap Sg^{-1}|$ and so $|S \cap Sg^{-1}| > \frac{1}{2} |G|$. Note that if $y \in S \cap Sg^{-1}$ then there is an $x \in S$ such that $y = xg^{-1}$ and $\varphi(y) = y^{-1}$. It follows then that $gy = \varphi(g^{-1}) \varphi(y^{-1}) = \varphi(g^{-1}y^{-1}) = \varphi((yg)^{-1}) = \varphi(x^{-1}) = x = yg$. Hence $S \cap Sg^{-1} \subseteq C(g)$, the centralizer of $g$ in $G$. Thus $|C(g)| \geq |S \cap Sg^{-1}| > \frac{1}{2} |G|$ and by Lagrange’s Theorem we conclude that $C(g) = G$ which means that $g \in Z(G)$ the center of $G$. Hence $S \subseteq Z(G)$ and so $|Z(G)| \geq |S| > \frac{3}{4} |G|$. By Lagrange’s Theorem once more, we are forced to conclude that $Z(G) = G$, fact that makes $G$ abelian. To finish the problem we claim that $S \subseteq G$: Clearly $e \in S$ and for $x, y \in S$ we have that $\varphi(xy^{-1}) = \varphi(x) \varphi(y^{-1}) = x^{-1}y = yx^{-1} = (xy)^{-1}$ establishing the fact that $xy^{-1} \in S$. By Lagrange’s theorem one more time, we conclude that $S = G$. ■