HOMEWORK 5: SOLUTIONS - MATH 341
INSTRUCTOR: George Voutsadakis

Problem 1 *(a) Show that $n^{19} - n$ is divisible by 21 for any integer n.*

(b) Find the remainder of 9^{1573} when divided by 11.

Solution:

(a) It suffices to show that $n^{19} - n = n(n^{18} - 1)$ is divisible by both 3 and 7.

If n is divisible by 3, then $n^{19} - n$ is also divisible by 3. If n is not divisible by 3, then $n \equiv 1$ or $n \equiv 2$ modulo 3. Therefore $n^2 \equiv 1$ modulo 3. Thus $n^{18} \equiv 1$ modulo 3, which implies $n^{18} - 1 \equiv 0$. Thus $n^{19} - n$ is divisible by 3.

If n is divisible by 7, then $n^{19} - n$ is also divisible by 7. If, on the other hand, n is not divisible by 7, then $(n, 7) = 1$, whence, by Euler's Theorem, $n^6 \equiv 1$ modulo 7. Thus, $n^{18} \equiv 1$ modulo 7, which gives $n^{18} - 1 \equiv 0$. Thus $n^{19} - n$ is divisible by 7.

(b) Since $(9, 11) = 1$, by Euler's Theorem, we get $9^{10} \equiv 1$ modulo 11. Therefore

$$\begin{aligned} 9^{1573} &= (9^{10})^{157} \cdot 9^3 \\ &\equiv 9^3 \\ &= 81 \cdot 9 \\ &\equiv 4 \cdot 9 \\ &= 36 \\ &\equiv 3, \end{aligned}$$

where all the congruences that appear above are assumed to be modulo 11.

■

Problem 2 *(a) Let H be a subgroup of a finite group G and K a subgroup of H. Suppose that the index $[G : H] = n$ and the index $[H : K] = m$. Show that the index $[G : K] = nm$. (Hint: Let x_iH be the distinct cosets of H in G and y_jK the distinct left cosets of K in H. Show that x_iy_jK are the distinct cosets of K in G.)*

(b) Let H and K be subgroups of a group G and for all $a, b \in G$ let $a \sim b$ if and only if $a = hbk$ for some $h \in H$ and $k \in K$. Show that the relation $\sim$ so defined is an equivalence relation. Describe the equivalence classes (which are called **double cosets***).*

Solution:

(a) Let $x_iH, i \in I$, be the distinct cosets of H in G and $y_jK, j \in J$, the distinct left cosets of K in H. We show that $x_iy_jK, i \in I, j \in J$, are the distinct cosets of K in G.

We first show that $x_iy_jK, i \in I, j \in J$, cover the entire group G. Suppose that $g \in G$. Then, since the $x_iH, i \in I$, are the distinct cosets of H in G, there exists $p \in I$ such

that $g \in x_pH$, i.e., there exists $h \in H$, such that $g = x_ph$. But $y_jK, j \in J$, are all the distinct cosets of K in H, whence there exists $q \in J$, such that $h \in y_qK$, i.e., there exists $k \in K$, such that $h = y_qk$. But then we have $g = x_ph = x_py_qk$, whence $g \in x_py_qK$, i.e., the sets $x_iy_jK, i \in I, j \in J$, cover G.

Finally, we need to show that the sets $x_iy_jK, i \in I, j \in J$, are disjoint. Suppose, to this end, that $x_iy_jK \cap x_py_qK \neq \emptyset$, for some $i, p \in I$ and $j, q \in J$. Then, there exist $k_1, k_2 \in K$, such that $x_iy_jk_1 = x_py_qk_2$. Since $y_jk_1 \in H$ and $y_qk_2 \in H$, this implies that $x_iH \cap x_pH \neq \emptyset$. But then, since $x_iH, i \in I$, are the distinct cosets of H in G, this yields that $i = p$. Thus, we have $x_iy_jk_1 = x_iy_qk_2$, whence, by the left cancellation property, $y_jk_1 = y_pk_2$. But this shows that $y_jK \cap y_qK \neq \emptyset$, which implies that $j = q$. Therefore, the sets $x_iy_jK, i \in I, j \in J$, are disjoint.

(b) Since $e \in H$ and $e \in K$, and, for all $a \in G$, $a = eae$, we have that $a \sim a$ and $\sim$ is reflexive. Now suppose that $a \sim b$. Then, there exist $h \in H$ and $k \in K$, such that $a = hbk$. But then $b = h^{-1}ak^{-1}$, with $h^{-1} \in H$ and $k^{-1} \in K$, because of the subgroup property. Therefore $b \sim a$ and $\sim$ is also symmetric. Finally, suppose that $a \sim b$ and $b \sim c$. Then, there exist $h_1, h_2 \in H$ and $k_1, k_2 \in K$, such that $a = h_1bk_1$ and $b = h_2ck_2$. Therefore $a = h_1h_2ck_1k_2$, where $h_1h_2 \in H$ and $k_1k_2 \in K$, by the subgroup property. Hence $a \sim c$ and $\sim$ is also transitive. Thus $\sim$ is indeed an equivalence relation on G.

To determine the equivalence class of $a \in G$ we work as follows:

$$\begin{aligned} [a] &= \{b \in G : b \sim a\} \\ &= \{b \in G : b = hak, \text{ for some } h \in H, k \in K\} \\ &= HaK. \end{aligned}$$

■

Problem 3 *Determine whether the following ϕ is a homomorphism and, in cases where it is, determine its kernel:*

(a) $\phi : \mathrm{GL}(2, \mathbb{R}) \to \mathbb{R}^*$, *where* $\mathrm{GL}(2, \mathbb{R})$ *is the general linear group of* 2×2 *invertible matrices and* $\phi(A) = \det(A)$.

(b) $\phi : \mathbf{Z}_7 \to \mathbf{Z}_2$, *where* $\phi(x) =$ *the remainder of* x mod 2.

Solution:

(a) Let $A, B \in \mathrm{GL}(2, \mathbb{R})$. Then we have

$$\phi(A \cdot B) = \det(A \cdot B) = \det(A) \cdot \det(B) = \phi(A) \cdot \phi(B).$$

Thus ϕ is in fact a homomorphism. For its kernel we get

$$\begin{aligned} \mathrm{Ker}(\phi) &= \{A \in \mathrm{GL}(2, \mathbb{R}) : \phi(A) = 1\} \\ &= \mathrm{SL}(2, \mathbb{R}). \end{aligned}$$

(b) This ϕ is not a homomorphism. Take for instance $3, 4 \in \mathbf{Z}_7$. We have

$$\phi(3+4) = \phi(0) = 0 \neq 1 + 0 = \phi(3) + \phi(4).$$

■

Problem 4 *(a) Find all possible homomorphisms from* $\mathbf{Z}$ *to* $\mathbf{Z}$.

(b) Find all possible homomorphisms from $\mathbf{Z}$ *onto* $\mathbf{Z}$.

Solution:

(a) All possible homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$ are determined by the image of the generator 1. So, suppose that $\phi(1) = n \in \mathbf{Z}$. Then the homomorphism is

$$\phi(k) = \phi(k \cdot 1) = k\phi(1) = kn,$$

for all $k \in \mathbf{Z}$. Hence all homomorphisms are $\phi_n : \mathbf{Z} \to \mathbf{Z}$, with $\phi_n(k) = kn$, for all $k \in \mathbf{Z}$, over different values of $n \in \mathbf{Z}$.

(b) From part (a), it suffices to take those ϕ_n's that map the generator 1 to a generator in $\mathbf{Z}$. But $\mathbf{Z}$ has only two generators 1 and -1. Therefore, the only two homomorphisms of $\mathbf{Z}$ onto $\mathbf{Z}$ are

$$\phi_1 : \mathbf{Z} \to \mathbf{Z}; \phi_1(k) = k,$$

$$\phi_{-1} : \mathbf{Z} \to \mathbf{Z}; \phi_{-1}(k) = -k.$$

■

Problem 5 *(a) Show that the dihedral group* D_4 *contains a subgroup isomorphic to the Klein 4-group* V.

(b) Let $G = \mathrm{GL}(2, \mathbf{Z}_2)$, *the general linear group of* 2×2 *invertible matrices with coefficients in* $\mathbf{Z}_2$. *Show that* $G \cong S_3$.

Solution:

(a) Let's let $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, -1 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, k = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, -k = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Then the multiplication table of V, the Klein four group, becomes

	1	-1	k	$-k$
1	1	-1	k	$-k$
-1	-1	1	$-k$	k
k	k	$-k$	1	-1
$-k$	$-k$	k	-1	1

Now consider also the subgroup of D_4 consisting of $H = \{\rho_0, \rho^2, \tau, \rho^2\tau\}$. Its multiplication table is

	ρ_0	ρ^2	τ	$\rho^2\tau$
ρ_0	ρ_0	ρ_2	τ	$\rho^2\tau$
ρ^2	ρ^2	ρ_0	$\rho^2\tau$	τ
τ	τ	$\rho^2\tau$	ρ_0	ρ^2
$\rho^2\tau$	$\rho^2\tau$	τ	ρ^2	ρ_0

Now it is obvious from the two multiplication tables that $V \cong H$, where the isomorphism $\phi : V \to H$ is given by

$$1 \mapsto \rho_0, -1 \mapsto \rho^2, k \mapsto \tau \text{ and } -k \mapsto \rho^2\tau.$$

(b) We present the two multiplication tables

	1	(12)	(13)	(23)	(123)	(132)
1	1	(12)	(13)	(23)	(123)	(132)
(12)	(12)	1	(132)	(123)	(23)	(13)
(13)	(13)	(123)	1	(132)	(12)	(23)
(23)	(23)	(132)	(123)	1	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	1
(132)	(132)	(23)	(12)	(13)	1	(123)

and, setting $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, j = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, k = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, a = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, b = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, we get the table

	1	i	j	k	a	b
1	1	i	j	k	a	b
i	i	1	b	a	k	j
j	j	a	1	b	i	k
k	k	b	a	1	j	i
a	a	j	k	i	b	1
b	b	k	i	j	1	a

Now it is obvious that the two groups are isomorphic via the isomorphism $\phi : \mathrm{GL}(2, \mathbf{Z}_2) \to S_3$ with

$$1 \mapsto 1, i \mapsto (12), j \mapsto (13), k \mapsto (23), a \mapsto (123) \text{ and } b \mapsto (132).$$

■