Exam 2 **Hamid Sagban**

May 19, 2009

(1) (a) For suppose not, then we would have $|f(a)| = k$ for some $k \in \mathbb{Z}^+$. Now $f(a^{k+1}) = f(a^k)\diamond f(a) = (f(a))^k \diamond f(a) = f(a)$, so that $a^{k+1} = a$ since f is injective. Thus $a^k = e$, a contradiction since $|a| = \infty$.

(b) Take $c \in M_2$. Since f is bijective, there is $a \in M_1$ such that $f(a) = c$. Now take $j \in f(H)$, thus $j = f(h_1)$ for some $h_1 \in H$. We have $c \diamond j = f(a) \diamond f(h_1) = f(a * h_1) = f(h_2 * a) = f(h_2) \diamond c$, for some $h_2 \in H$. Since $f(h_2) \in f(H)$, the conclusion follows.

(c) Let $y \in A = \{a_1, a_2, \ldots, a_k\} \subseteq M_1$. Then $(f(y))^m = f(y^m) = f(b)$; distinctness of these solutions follows from the injectivity of f. Now suppose $d^m = f(b)$, with $d = f(a)$ for some $a \in M_1$. Then $d^m = f(b) \implies f(a)^m \diamond (f(b))^{-1} = e_{m_2} \implies f(a^m) \diamond f(b^{-1}) = e_{m_2} \implies f(a^m * b^{-1}) = f(e_{m_1})$, so that $a^m * b^{-1} = e_{m_1}$, and thus $a^m = b$. We know $a \in A$, and thus $d \in f(A)$.

(2) We know $U(Z_9) = \{1, 2, 4, 5, 7, 8\}$ under $\times_9$, and $(Z_3, +_3) \oplus (Z_2, +_2) = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}$. Since $|2| = 6$, we have $U(Z_9) = \langle 2 \rangle$, and thus $(U(Z_9), \times_9) \cong (Z_6, +_6)$. Also, we have $(Z_3, +_3) \oplus (Z_2, +_2) = \langle (1,1) \rangle$, so we have $(Z_3, +_3) \oplus (Z_2, +_2) \cong (Z_6, +_6)$. Thus $(U(Z_9), \times_9) \cong (Z_3, +_3) \oplus (Z_2, +_2)$. The possibilities for $f(2)$ are $(1,1)$ and $(2,1)$.

(3) Let $f : U(Z_8) \to U(Z_{12})$. Define f explicitly such that $f(1) = 1, f(7) = 7, f(5) = 5, f(3) = 11$. Well-definition can be seen from the mapping. Clearly f is injective by construction. Also, for each $b \in U(Z_{12})$, we have an $a \in U(Z_8)$ such that $f(a) = b$. It remains to show homomorphism. Since the function is defined explicitly, we show this explicitly:

$f(1 \times_8 1) = f(1) = 1 = f(1) \times_{12} f(1)$

$f(1 \times_8 3) = f(3) = 11 = f(1) \times_{12} f(3)$

$f(1 \times_8 5) = f(5) = 5 = f(1) \times_{12} f(5)$

$f(1 \times_8 7) = f(7) = 7 = f(1) \times_{12} f(7)$

$f(3 \times_8 3) = f(1) = 1 = f(3) \times_{12} f(3)$

$f(3 \times_8 5) = f(7) = 7 = f(3) \times_{12} f(5)$

$f(3 \times_8 7) = f(5) = 5 = f(3) \times_{12} f(7)$

$f(5 \times_8 5) = f(1) = 1 = f(5) \times_{12} f(5)$

$f(5 \times_8 7) = f(3) = 11 = f(5) \times_{12} f(7)$

$f(7 \times_8 7) = f(1) = 1 = f(7) \times_{12} f(7)$ and we are done.

(4) To show well definition, we have to show $a = b$ implies $f(a) = f(b)$ for all $a, b \in M$. We know $a = b$, so we have $a * b^{-1} = e$, thus $(a * b^{-1}) * (a * b^{-1})^{n-1} = e * (a * b^{-1})^{n-1} \implies a^n * b^{-n} = e$ so $a^n = b^n$ and we are done. To show one-to-one, we have to show $f(a) = f(b)$ implies $a = b$ for all $a, b \in M$. Thus we have $a^n = b^n \implies a^n * b^{-n} = (a * b^{-1})^n = e$. Suppose for some arbitrary k, we have $k^n = e$. Thus $|k| \mid n$, and we know $|k| \mid m$. But since $\gcd(n, m) = 1$, $|k| = 1$, and we have $k = e$. So $a * b^{-1} = e$, and thus $a = b$. Onto follows since the mapping is from a set to itself. Now we have to show $f(a * b) = f(a) * f(b)$ for all $a, b \in M$. We have $f(a * b) = (a * b)^n = a^n * b^n = f(a) * f(b)$ and we are done.

(5) We have $\langle a^{10} \rangle \cap \langle a^{21} \rangle = \{a^{14}, a^{28}\}$. Thus $H = \langle a^{14} \rangle$ and of order 2. Now $\langle a \rangle / \langle a^{14} \rangle = \{\{a, a^{15}\}, \{a^2, a^{16}\}, \{a^3, a^{17}\}, \{a^4, a^{18}\}, \{a^5, a^{19}\}, \{a^6, a^{20}\}, \{a^7, a^{21}\}, \{a^8, a^{22}\}, \{a^9, a^{23}\}, \{a^{10}, a^{24}\}, \{a^{11}, a^{25}\}, \{a^{12}, a^{26}\}, \{a^{13}, a^{27}\}, \{a^{14}, a^{28}\}\}$, the order of whose elements are 14, 7, 14, 7, 14, 7, 2, 7, 14, 7, 14, 7, 14, and 1, respectively. Since $|\langle a \rangle / \langle a^{14} \rangle| = 14 = 7 \times 3$, then by the exam question, $\langle a \rangle / \langle a^{14} \rangle$ is a cyclic subgroup of order 14. Thus $\langle a \rangle / \langle a^{14} \rangle \cong \mathbb{Z}_n$ for $n = 14$ by the theorem proved in class.

For the latter part of the question, finding m amounts to finding the $\text{lcm}(21, 15)$, which is 105. Thus $21\mathbb{Z} \cap 15\mathbb{Z} = 105\mathbb{Z}$, and we are done.

(6) Since $10Z$ is group-isomorphic to Z, it suffices to construct a mapping f from $(\mathbb{Q}^*, \times)$ to $(\mathbb{Z}, +)$ such that $image(f) = Z$. First, let $k(x)$ denote the number of all prime factors of x; suppose $x = p_1^{q_1} p_2^{q_2} \ldots p_n^{q_n}$ for some primes $p_1, p_2, \ldots, p_n$. Then $k(x) = q_1 + q_2 + \ldots + q_n$. By default, let $k(\pm 1) = 0$ since 1 has no prime factors. Also, the fundamental theorem of arithmetic guarantees well-definition of $k(x)$.

Now our mapping is defined as such: take $\frac{a}{b} \in \mathbb{Q}^*$. Then $f(\frac{a}{b}) = k(a) - k(b)$. Take $x, y \in \mathbb{Q}^*$, we show $f(xy) = f(x) + f(y)$. Since $x, y \in \mathbb{Q}^*$, we have $x = \frac{a}{b}$ and $y = \frac{c}{d}$, for some $a, b, c, d \in \mathbb{Z}^*$. Thus $f(xy) = f(\frac{a}{b} \times \frac{c}{d}) = f(\frac{ac}{bd}) = k(ac) - k(bd) = k(a) + k(c) - k(b) - k(d)$. Also, $f(x) + f(y) = f(\frac{a}{b}) + f(\frac{c}{d}) = k(a) - k(b) + k(c) - k(d)$, and thus we have a group homomorphism that is not trivial. For completeness, we show well-definition of f. Suppose $\frac{a}{b} = \frac{c}{d}$, we have to show $f(\frac{a}{b}) = f(\frac{c}{d})$. From $\frac{a}{b} = \frac{c}{d}$, we have $ad = bc$, so that $k(ad) = k(bc)$. Hence $k(a) + k(d) = k(b) + k(c)$. That is, $k(a) - k(b) = k(c) - k(d)$, and thus $f(\frac{a}{b}) = f(\frac{c}{d})$. We provide an example. Take $\frac{10}{3} \in \mathbb{Q}^*$, then $f(\frac{10}{1} \times \frac{1}{3}) = f(\frac{10}{1}) + f(\frac{1}{3}) = k(10) - k(1) + k(1) - k(3) = 2 - 0 + 0 - 1 = 1$, whereas $f(\frac{10}{3}) = k(10) - k(3) = 2 - 1 = 1$.

(7) **Solved by Ayman**: Since $H = \{1, -1\}$ is the only nontrivial finite subgroup of $(Q^*, \times)$ and $Z/2Z$ is group- isomorphic to H, we will construct a group homomorphism f from $(Z, +)$ into $(Q^*, \times)$ such that $Ker(f) = 2Z$. Define $f : (Z, +) \to (Q^*, \times)$ such that $f(even) = 1$ (note 0 is an even number) and $f(odd) = -1$. It is easy to check that f is a group-homomorphism from Z into Q^*. Since H is the only finite subgroup of $(Q^*, \times)$, we conclude that there are no other nontrivial group-homomorphisms from Z into Q^*.

(8) $|(1,0)| = 1$, $|(1,1)| = 2$, $|(5,0)| = 2$, $|(5,1)| = 2$, $|(7,0)| = 2$, $|(7,1)| = 2$, $|(11,0)| = 2$, $|(11,1)| = 2$.

(9) We first prove an auxilary result: take $a, b \in \mathbb{Z}^+$ such that $a \neq b$, then $\frac{1}{a} + \mathbb{Z} \ \cap \ \frac{1}{b} + \mathbb{Z} = \{\}$. Suppose not, then there is a q such that $q \in \frac{1}{a} + \mathbb{Z}$ and $q \in \frac{1}{b} + \mathbb{Z}$. Thus we have $q = \frac{1}{a} + c$ and $q = \frac{1}{b} + d$, for some $c, d \in \mathbb{Z}$. We have $\frac{1}{a} + c = \frac{1}{b} + d$, so that $\frac{1}{a} = \frac{1}{b} + (d - c) \implies \frac{1}{a} \in \frac{1}{b} + \mathbb{Z}$. The only element between 0 and 1 in $\frac{1}{b} + \mathbb{Z}$ is $\frac{1}{b}$, so we must have $\frac{1}{a} = \frac{1}{b}$, a contradiction.

Now suppose there are finitely many elements in $\mathbb{Q}/\mathbb{Z}$, then we have $[\mathbb{Q} : \mathbb{Z}] = m$ for some $m \in \mathbb{Z}^+$. Take the following m number of elements:

$$1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{m}$$

each of which is a representative of distinct left cosets by the auxiliary result proved previously. But then $\frac{1}{m+1} + \mathbb{Z}$ is another distinct left coset, contradiction.

Take $x \in \mathbb{Q} - \mathbb{Z}$. Then $x + \mathbb{Z}$ is a left coset of $\mathbb{Z}$. Now take the minimum of $x + \mathbb{Z}$, and call it y. Then $y = \frac{a}{b}$ such that $\gcd(a, b) = 1$. Thus we have $|x + \mathbb{Z}| = |y + \mathbb{Z}| = |\frac{a}{b} + \mathbb{Z}| = b$, since b is the least number such that $(\frac{a}{b})^b \in \mathbb{Z}$. Therefore, all elements of $\mathbb{Q}/\mathbb{Z}$ are of finite order.

(10) We know $M_1/\mathrm{Ker}(f)$ is isomorphic to $\mathbb{Z}_6$. Thus $|M_1/\mathrm{Ker}(f)| = 6$, so that $|\mathrm{Ker}(f)| = 5$. Take $a \neq e \in \mathrm{Ker}(f)$. Then $|a| = 5$. Since there is a b such that $f(b) = 1$, we have $|1| \mid |b|$, thus $6 \mid |b|$. Therefore, $|b|$ is either 6 or 30. If it is 30, we are done. Otherwise assume $|b| = 6$. Then $|a * b| = 30$, and we are done.