Math 307 Abstract Algebra Homework 7 **Sample solution**

Based on the solution of Jacopo Gliozzi

1. If r is a divisor of m and s is a divisor of n, find a subgroup of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ that is isomorphic to $\mathbb{Z}_r \oplus \mathbb{Z}_s$.

   Solution. Let $a = \frac{m}{r}$ and $b = \frac{n}{s}$. Then $H = \langle a \rangle \leq \mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_r$ and $H_2 = \langle b \rangle \leq \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_s$. Then $H = H_1 \oplus H_2 = \{(x, y) \in \mathbb{Z}_m \oplus \mathbb{Z}_n : x \in H_1, y \in H_2\}$ is isomorphic to $\mathbb{Z}_r \oplus \mathbb{Z}_s$.

   [In general, it is easy to prove that if $H_1 \cong K_1, H_2 \cong K_2$, then $H_1 \oplus H_2 \cong K_1 \oplus K_2$.]

2. (a) What is the order of the element $14 + \langle 8 \rangle$ in $\mathbb{Z}_{24}/\langle 8 \rangle$?

   Solution. We must find the smallest m such that $14m \in \langle 8 \rangle = \{8k, k \in \mathbb{Z}\}$. The number $14m$ will then be the least common multiple of 8 and 14, and $m = \text{lcm}(8, 14)/14 = 56/14 = 4$.

   (b) What is the order of $4U_5(105)$ in the factor group $U(105)/U_5(105)$.

   Solution. We must find the smallest m such that $4^m \in U_5(105)$, so 4^m must be relatively prime to 105 and $4^m = 5k + 1, 0 \leq k \leq 20$. $105 = 3 * 5 * 7$, and $4^m = 2^{2m}$, so 4^m will always be relatively prime to 105 because they share no common factors. We must then find the smallest m such that $4^m = 5k + 1$. For $m = 1$ we $4 \neq 1 \mod 5$, but for $m = 2$ we have $4^2 = 16 = 5(3) + 1 \in U_5(105)$, so $|4U_5(105)| = 2$.

3. Let $G = \mathbb{Z}_4 \oplus U(4)$, $H = \langle (2, 3) \rangle$ and $K = \langle (2, 1) \rangle$. Show that $G/H \ncong G/K$.

   Solution. Note that $G = \{(0, 1), (0, 3), (1, 1), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\}$. Each G/K and G/H has four elements. We label the cosets of H as: $G/H = \{H, (1, 1)H, (2, 1)H, (3, 1)H\}$. It is easy to see that the coset $(1, 1)H$ has order 4 and will generate the factor group, so G/H is cyclic. On the other hand, we can label the cosets of K as $G/K = \{K, (0, 3)K, (1, 1)K, (1, 3)K\}$, yet all the elements except the identity have order two, so none of them can generate the group and G/K is not cyclic. Therefore $G/H \ncong G/K$.

4. Let G be a finite group, and H be a normal subgroup of G.

   (a) Show that the order of aH in G/H must divide the order of a in G.

   Solution. (a) Suppose a has order n. Then $a^n = e \in G$. Then $(aH)^n = a^n H = eH = H$. So, the order of aH must be a factor of n. [Here we use the fact that if x is a group satisfies $x^n = e$, then the order of x divides n.

   (b) Show that it is possible that $aH = bH$, but $|a| \neq |b|$.

   Solution. Let G be any group with more than one elements. Then there is only one element of order 1 in G, namely, e. However, if we let $H = G$, then $G/H = \{H\}$ so that $aH = H$ has order 1 for every $a \in G$.

5. If G is a group and $|G : Z(G)| = 4$, prove that $G/Z(G)$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

   Solution. Every four element subgroup is either isomorphic to $\mathbb{Z}_4$ (a cyclic group) or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (the Klein 4-Group). Because there are only two options, assume the opposite, that $G/Z(G) \cong \mathbb{Z}_4$. We then know that $G/Z(G)$ is cyclic because $\mathbb{Z}_4$ is. From a previously proved theorem, if a factor group is cyclic then the overall group is Abelian so G must be Abelian. However, if this were the case, then the center $Z(G) = G$, and $|G/Z(G)| = |G/G| = |G|/|G| = 1$ which

contradicts our assumption that is is four. Our factor group must then be isomorphic to the Klein 4-Group.

6. Suppose that $N \triangleleft G$ and $|G/N| = m$, show that $x^m \in N$ for all $x \in G$.

   Solution. Because $N \triangleleft G$, the factor group G/N is well-defined, and it is the collection of the cosets of N in G. For all $x \in G$, $xN \in G/N$. The order of the group G/N is m, and because the order of any element must divide the order of the group, $(xN)^m = e = N$ (the identity in a factor group is the subgroup with which it is defined). We then have that $(xN)^m = x^m N = M$, which implies that $x^m n = n_1 \in N \ \forall n \in N$, so $x^m = n_1 n^{-1} \in N$ by closure and existence of an inverse and $x^m \in N$.

7. (a) Let $G = \{3^a 6^b 10^c : a, b, c \in \mathbb{Z}\}$ under multiplication. Show that G is isomorphic to $\langle 3\rangle \times \langle 6\rangle \times \langle 10\rangle$.

   Solution. Consider the subgroups $H = \langle 3\rangle$ and $K = \langle 6\rangle$, they are normal subgroups because G is Abelian, so we can apply the theorem that states that a subgroup of G defined by $M = HK$ is isomorphic to direct product of H and K if their intersection is the identity and $M = HK$. $M = HK$ by definition, and if $\exists f \in H \cap K$ then $f = 3^a = 6^b$, which is only true for integers $a = b = 0$, giving us $f = e$. Furthermore, the identity will always be in subgroup (union of subgroups is a subgroup). Therefore $H \cap K = \{e\}$ and $M \cong H \times K$. Now consider the subgroup $L = \langle 10\rangle$, we have that $G = HKL = ML$. Now if $\exists s \in M \cap L$ then $s = 3^a 6^b = 10^c$, which can only be true for $a = b = c = 0$, so $s = e$. Additionally, the identity is always in a subgroup, implying that $M \cap L = \{e\}$. Therefore $G \cong M \times L \cong H \times K \times L$.

   (b) Let $H = \{3^a 6^b 12^c : a, b, c \in \mathbb{Z}\}$ under multiplication. Show that G is NOT isomorphic to $\langle 3\rangle \times \langle 6\rangle \times \langle 12\rangle$.

   Solution. We know that $M \cong H \times K$, yet when we try to show the analogous thing for the direct product of M and $\langle 12\rangle$ we arrive at a problem because $3^{-1}6^2 = 12 \in M \cap \langle 12\rangle$ and 12 is not the identity, Therefore G cannot be isomorphic to $\langle 3\rangle \times \langle 6\rangle \times \langle 12\rangle$.

8. (Extra credits) (a) (5 points) Show that $U(2^3) = \langle 7\rangle \oplus \langle 3\rangle$, $U(2^4) = \langle 15\rangle \oplus \langle 3\rangle$.

Solution. In the Abelian group $U(2^3) = U(8) = \{1, 3, 5, 7\}$, $H_1 = \langle 7\rangle = \{1, 7\}$ and $H_2 = \langle 3\rangle = \{1, 3\}$ are normal subgroups. Clearly, $H_1 \cap H_2 = \{1\}$. So, $U(16) \cong H_1 \times H_2 \cong H_1 \oplus H_2$.

In the Abelian group $U(2^4)$, $H_1 = \langle 15\rangle = \{1, 15\}$ and $H_2 = \langle 3\rangle = \{1, 3, 9, 11\}$ are normal subgroups. Clearly, $H_1 \cap H_2 = \{1\}$. So, $U(16) \cong H_1 \times H_2 \cong H_1 \oplus H_2$.

(b) (5 points) Show that $U(2^m) = \langle 2^m - 1\rangle \oplus \langle 3\rangle$.

Solution. Suppose $n > 3$. Note that $U(2^n) = \{1, 3, 5, \ldots, 2^n - 1\}$ has 2^{n-1} elements. Let $H_1 = \langle 2^n - 1\rangle = \{2^n - 1, 1\}$. Consider $H_2 = \langle 3\rangle$. We prove that $|3| = 2^{n-2}$ in $U(2^n)$. Note that the order of 3 divides the order of $U(2^n)$ and must be of the form 2^m. We claim that for $m \geq 1$, we have the following.

$$P(m)\text{: } 3^{2^m} + 1 = 2\mu_m \text{ and } 3^{2^m} - 1 = 2^{m+2}\eta_m \text{ for some odd numbers } \mu_m, \eta_m.$$

When $m = 2$, $3^2 - 1 = 8 = 2^3 1$, $3^2 + 1 = 2 \cdot 5$. Suppose the result holds for some $m \geq 1$. Consider $3^{2^{m+1}} + 1 = (3^{2^m})^2 + 1 = (2\mu_m - 1)^2 + 1 = 4\mu_m^2 - 4\mu_m + 2 = 2(2\mu_m^2 - 2\mu_m + 1) = 2\mu_{m+1}$ such that $\mu_{m+1} = 2(\mu_m^2 - \mu_m) + 1$ is odd, and $3^{2^{m+1}} - 1 = (3^{2^m} - 1)(3^{2^m} + 1) = 2^{m+2}\eta_m 2\mu_m = 2^{m+3}\eta_{m+1}$ such that $\eta_{m+1} = \mu_m\eta_m$ is odd.

As a result, we see that $3^{2^{n-3}} = 2^{n-1}\eta_{n-3} + 1 \neq 1 \in U(2^n)$ and and $3^{2^{n-2}} = 2^n\eta_{n-2} + 1 = 1 \in U(2^n)$. Also, $2^n - 1 \notin H_2$. Else, we will have $3^{2^{n-3}} = -1$ so that $(3^{2^{n-3}})^2 = 3^{2^{n-2}} = 1$, but it is not the case as $3^{2^{n-3}} + 1 = 2\mu_{n-3} \neq 0 \in Z_{2^n}$. Hence, $U(2^n) = H_1 \times H_2 \cong H_1 \oplus H_2$.

9. Suppose s, t are relatively prime. Prove that $U_t(st)$ is isomorphic to $U(s)$. [Hint: $U_t(st) = \{kt + 1 \in U(st) : k = 0, \ldots, s - 1\}$.]

Solution. Consider the mapping $\phi : U_t(st) \mapsto U(s), \phi(x) = [x]_s$.
Well-defined: for every $x \in U_t(st)$, because x shares no common divisors with st, it will share no common divisors with s, and $\gcd(x, s) = 1$. Because the greatest common divisor is conserved through the Euclidean algorithm, and we can write $x = qs + [x]_s, 0 \leq [x]_s \leq s - 1$, and $\gcd(x, s) = 1 = \gcd([x]_s, s)$. Therefore $[x]_s \in U(s)$.
One-to-One: If $\phi(x) = \phi(y) = [x]_s = [y]_s$, then $x - y$ is divisible by s. Also, $x = kt + 1$ and $y = mt + 1$ so that $x - y$ is divisible by t. Since s, t are relatively prime, we see that $x - y$ is divisible by st and are equal in $U(st)$ and hence equal in $U_t(st)$. Onto: Consider an element $y \in U(s)$. We aim at finding $x = tq + 1 \in U(st)$ such that $f(x) = [x]_s = y \in U(s)$. That is, $[y]_s = [tq + 1]_s = [t]_s[q]_s + [1]_s$ so that $[t]_s[q]_s = [y - 1]_s$. Since $\gcd(s, t) = 1$, $[t]_s \in U(s)$ so that $[q]_s = [t]_s^{-1}[y - 1]_s$. Thus, we can choose $q \in \{0, 1, \ldots, s - 1\}$ such that $[q]_s \in U(s)$ and $x = qt + 1$. Because y shares no common factors with s and t, it will share no factors with their product, so $\gcd(y, st) = 1$. Then $x \in U_t(st)$ such that $f(x) = [y]_s$.
Operation Preserving: $\phi(xy) = [xy]_s = [x]_s[y]_s = \phi(x)\phi(y)$ by multiplication of congruence classes.