## Solutions to Homework 7

**Problem 1.** a) List all abelian groups of order 4225 (up to isomorphism).

b) Let $m, n$ be positive integers and let $d = \gcd(m, n)$ and $l = \text{lcm}(m, n)$. Prove that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_d \times \mathbb{Z}_l$. Hint: do this first when $d = 1$ (we basically did it in class), then use factorization into prime powers of $m, n, d, l$ and rearrange. It may be helpful to work out the case when $m = 540$ and $n = 600$ first.

**Solution.** a) Recall first the Fundamental Theorem of Finite Abelian Groups

**Fundamental Theorem of Finite Abelian Groups.**
1) If $G$ is a finite abelian group of order $n = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$, where $p_1 < \dots < p_t$ are prime numbers, then $G$ has unique subgroup $P_i$ of order $p_i^{s_i}$, $i = 1, \dots, t$ and

$$G \cong P_1 \times P_2 \times \dots \times P_t.$$

2) If $P$ is a finite abelian group of order $p^m$, $p$ a prime, then

$$P \cong \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \dots \times \mathbb{Z}_{p^{m_k}}$$

for some $m_1 \geq m_2 \geq \dots \geq m_k \geq 1$ such that $m_1 + \dots + m_k = m$. Moreover, the numbers $m_1, m_2, \dots, m_k$ are unique for $P$.

Let $G$ be an abelian group of order 4225. Note that $4225 = 5^2 \cdot 13^2$. By part a) of the FTFAG, $G$ has unique subgroups $P_1, P_2$ of orders $5^2, 13^2$ respectively and $G \cong P_1 \times P_2$. We need to find out all the possibilities for $P_1$ and $P_2$. Since 2 has two partitions: 2 and $1 + 1$, there are exactly two abelian groups of order $p^2$ for any prime number $p$: $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$. It follows that we have four possibilities for $G$:

$$\mathbb{Z}_{25} \times \mathbb{Z}_{169}; \quad \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{169}; \quad \mathbb{Z}_{25} \times \mathbb{Z}_{13} \times \mathbb{Z}_{13}; \quad \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{13} \times \mathbb{Z}_{13}.$$

**Remark.** We will show later that every group of order 4225 is abelian. We already know from Problem 7 in homework 6 that every group of order $p^2$ is abelian for any prime $p$.

b) We proved in class that if $gcd(m, n) = 1$ then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ (see also part 7) of problem 7 in homework 4).

Let us first work out the case when $m = 540 = 2^2 \cdot 3^3 \cdot 5$ and $n = 600 = 2^3 \cdot 3 \cdot 5^2$. Thus

$$\mathbb{Z}_{540} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5 \text{ and } \mathbb{Z}_{600} \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}.$$

Thus

$$\mathbb{Z}_{540} \times \mathbb{Z}_{600} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}.$$

Rearranging the factors we see that

$$\mathbb{Z}_{540} \times \mathbb{Z}_{600} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{5^2}.$$

Now

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{2^2 \cdot 3 \cdot 5} = \mathbb{Z}_{60} = \mathbb{Z}_{\gcd(540,600)}$$

and

$$\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_{2^3.3^2.5^2} = \mathbb{Z}_{1800} = \mathbb{Z}_{\mathrm{lcm}(540,600)}.$$

It follows that

$$\mathbb{Z}_{540} \times \mathbb{Z}_{600} \cong \mathbb{Z}_{60} \times \mathbb{Z}_{1800} = \mathbb{Z}_{\gcd(540,600)} \times \mathbb{Z}_{\mathrm{lcm}(540,600)}.$$

The general case is based on the same argument. Write

$$m = p_1^{s_1} \dots p_k^{s_k}, \quad n = p_1^{t_1} \dots p_k^{t_k},$$

where $p_1 < \ldots < p_k$ are primes and $s_i, t_j$ are non-negative integers. Then

$$\gcd(m,n) = p_1^{\min(s_1,t_1)} \dots p_k^{\min(s_k,t_k)} \text{ and } \mathrm{lcm}(m,n) = p_1^{\max(s_1,t_1)} \dots p_k^{\max(s_k,t_k)}.$$

It follows that

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{s_1}} \times \mathbb{Z}_{p_2^{s_2}} \times \ldots \times \mathbb{Z}_{p_k^{s_k}}, \quad \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{t_1}} \times \mathbb{Z}_{p_2^{t_2}} \times \ldots \times \mathbb{Z}_{p_k^{t_k}},$$

$$\mathbb{Z}_{\gcd(m,n)} \cong \mathbb{Z}_{p_1^{\min(s_1,t_1)}} \times \mathbb{Z}_{p_2^{\min(s_2,t_2)}} \times \ldots \times \mathbb{Z}_{p_k^{\min(s_k,t_k)}},$$

$$\mathbb{Z}_{\mathrm{lcm}(m,n)} \cong \mathbb{Z}_{p_1^{\max(s_1,t_1)}} \times \mathbb{Z}_{p_2^{\max(s_2,t_2)}} \times \ldots \times \mathbb{Z}_{p_k^{\max(s_k,t_k)}}.$$

We see that the cyclic factors of prime power orders in $\mathbb{Z}_m \times \mathbb{Z}_n$ and $\mathbb{Z}_{\gcd(m,n)} \times \mathbb{Z}_{\mathrm{lcm}(m,n)}$ are the same, just in different order, so indeed the groups $\mathbb{Z}_m \times \mathbb{Z}_n$ and $\mathbb{Z}_{\gcd(m,n)} \times \mathbb{Z}_{\mathrm{lcm}(m,n)}$ are isomorphic.

**Problem 2.** Call a group $G$ an H-group if every subgroup of $G$ is normal in $G$.

a) Show that any subgroup of an H-group is also an H-group.

b) Let $G$ be an H-group and $f : G \longrightarrow K$ a surjective homomorphism. Prove that $K$ is an H-group.

c) Let $G$ and $H$ be groups with no elements of infinite order (such groups are called **torsion**). Suppose that for any $a \in G$ and $b \in H$ the orders of $a$ and $b$ are relatively prime. Let $T$ be a subgroup of $G \times H$. Prove that $T = A \times B$ for a subgroup $A$ of $G$ and a subgroup $B$ of $H$. Prove that $T$ is normal if and only if both $A$ and $B$ are normal in $G$, $H$ respectively.

d) In part c) assume that both $G$ and $H$ are H-groups. Prove that $G \times H$ is an H-group.

**Solution.** a) Let $B$ be a subgroup of an H-group $G$. Let $A$ be a subgroup of $B$. Then $A$ is also a subgroup of $G$, so $A$ is normal in $G$. Clearly this implies that $A$ is normal in $B$. Thus $B$ is an H-group.

b) We proved in class a result called **the correspondence theorem** (see the notes to the lecture on 10/02/26). It implies that if $f$ is a surjective homomorphism and $M$ is a normal subgroup in $G$ then $f(M)$ is normal in $K$. Let $L$ be a subgroup of $K$. Then $f^{-1}(L)$ is a subgroup of $G$ corresponding to $L$. Since $G$ is an H-group, $f^{-1}(L)$ is normal in $G$ and therefore $L = f(f^{-1}(L))$ is normal in $K$. This shows that $K$ is an H-group.

c) Take an element $(a,b) \in T$. Let $m$ be the order of $a$ and $n$ the order of $b$, so $\gcd(m,n) = 1$. We see that $(a,b)^m = (e,b^m) \in T$ Note that the order of $b^m$ is $n$, since $\gcd(m,n) = 1$. Thus the cyclic groups $< b^m >$ and $< b >$ have the same order and the first one is contained in the second. Thus they coincide: $< b^m >=< b >$. Thus $b = (b^m)^l$ for some $l$. It follows that $(a,b)^{ml} = (e,b) \in T$. Then $(a,e) = (a,b)(e,b)^{-1} \in T$ as well. We showed that if $(a,b) \in T$ then both $(a,e)$ and $(e,b)$ are in $T$. Let $A = \{a \in G : (a,e) \in T\}$, $B = \{b \in H : (e,b) \in T\}$. Thus we showed that $T \subseteq A \times B$. It is straightforward to verify that $A < G$ and $B < H$. Clearly $A \times B \subseteq T$ as $(a,b) = (a,e)(e,b)$. Thus $T = A \times B$. Since $(g,h)(a,b)(g,h)^{-1} = (gag^{-1}, hbh^{-1})$, it is clear that $A \times B$ is normal in $G \times H$ if and only if $A \lhd G$ and $B \lhd H$.

d) Suppose both $G$ and $H$ in c) are H-groups. If $T$ is a subgroup of $G \times H$ then $T = A \times B$ for some $A < G$, $B < H$. Then $A \lhd G$ and $B \lhd H$, so $T = A \times B \lhd G \times H$.

**Problem 3.** a) Let $G$ be a group and $a, b$ elements in $G$ such that the cyclic subgroups $< a >$ and $< b >$ are normal in $G$. Prove that if $< a >$ has infinite order then either $ba = ab$ or $ba = a^{-1}b$. Then prove that the latter case is not possible, i.e. $a$ and $b$ must commute.

b) Let $G$ be an H-group which has an element of infinite order. Prove that $G$ is abelian.

Let $G$ be a nonabelian H-group. Thus by b) each element in $G$ has finite order.

c) Suppose that $a, b \in G$ have odd order. Prove that $ab$ also has odd order. Hint: prove that the subgroup $< a >< b >$ has odd order. Conclude that the set $T$ of all elements of odd order in $G$ is a subgroup.

d) Suppose that $a, b \in G$ have order which is a power of 2. Prove that the order of $ab$ is also a power of 2. Conclude that the set $D$ of all elements in $G$ whose order is a power of 2 is a subgroup.

e) Prove that $G \cong D \times T$.

f) Conversely, suppose that $D$ is an H-group in which the order of every element is a power of 2 and $T$ is an H-group in which every element has odd order. Show that $D \times T$ is an H-group (use problem 2d)).

**Solution.** a) Note that an infinite cyclic group $< a >$ has exactly two generators: $a$ and $a^{-1}$. Since $< a >$ is normal in $G$, conjugation by $b$ is an automorphism of $< a >$ and therefore it maps any generator to a generator. Thus $bab^{-1}$ is either $a$ or $a^{-1}$. Suppose that $bab^{-1} = a^{-1}$. Then $ba^2b^{-1} = a^{-2}$ and $aba^{-1} = ba^{-2}$. Since $< b >$ is normal, we have $aba^{-1} \in < b >$, so $ba^{-2} \in < b >$. This implies that $a^2 \in < b >$ and therefore $a^2$ and $b$ commute. This contradicts the fact that $ba^2b^{-1} = a^{-2} \neq a^2$. Thus $bab^{-1} = a^{-1}$ is not possible and therefore $a$ and $b$ commute.

b) Let $G$ be an H-group and $a \in G$ be of infinite order (it exists). By part a), $a$ commutes with every element in $G$, i.e. $a \in Z(G)$. Thus $Z(G)$ contains all elements in $G$ of infinite order. If $b \in G$ is of finite order then $ab$ is also of infinite order (since $a$ and $b$ commute). We see that $a$ and $ab$ are in $Z(G)$. Since the center is a subgroup, $b = a^{-1}(ab) \in Z(G)$. We proved that $G = Z(G)$, so $G$ is abelian.

b) We proved in part b) of Problem 1 in homework 6 that if $H$, $K$ are finite subgroups of a group $G$ then $|HK| = |H||K|/|H \cap K|$ (problem 1 assumed that $G$ is finite but the

solution only uses the fact that $H$ and $K$ are finite). It follows that $|HK|$ divides the $|H||K|$.

Let $a, b \in G$ have both odd order. Since $G$ is an H-group, $< a >, < b >$ are normal subgroups and therefore $K =< a >< b >$ is a subgroup of $G$. The order of $K$ divides $| < a > || < b > |$. Since the orders of $a$ and $b$ are odd, $K$ has odd order. Since $ab \in K$, the order of $ab$ divides $|K|$, so it is odd. Thus the set $T$ is closes under multiplication. Clearly $e \in T$ and if $a$ has odd order the so does $a^{-1}$, so $T$ is closed under inversion. Thus $T$ is a subgroup of $G$.

d) Let $a, b \in G$ have order a power of 2. As in part c) we see that the group $K =< a >< b >$ has order a power of 2. It follows that $ab$ has order a power of 2. As in c) we conclude that $D$ is a subgroup of $G$.

e) Clearly $T$ and $D$ are normal subgroups of $G$ and $T \cap G = \{e\}$. Thus $TD = DT \cong D \times T$. Let $g \in G$. Then $g$ has finite order, say $2^m n$, where $n$ is odd. Then $g^{2^m}$ has order $n$, so $g^{2^m} \in T \subseteq TD$. Similarly $g^n \in D \subseteq TD$. Thus both $g^{2^m}$ and $g^n$ are in $TD$. Since $2^m$ and $n$ are relatively prime, we see that $g \in TD$. This shows that $G = TD$ and therefore $G \cong D \times T$.

f) This is an immediate consequence of problem 2d.

**Problem 4.** Let $G$ be a finite group and $p$ a prime number such that $p||G|$. Consider the set $S$ of all $p-$tuples $(a_1, ..., a_p)$ of elements from $G$ such that $a_1 a_2 ... a_p = e$, i.e.

$$S = \{(a_1, ..., a_p) : a_i \in G \text{ for all } i, \text{ and } a_1 ... a_p = e\}$$

Let $C$ be a cyclic group of order $p$ and $f$ a generator for $C$. We define an action of $C$ on $S$ as follows: if $s \in C$ then $s = f^i$ for a unique $0 \leq i < p$ and we set $s * (a_1, ..., a_p) = (a_{i+1}, a_{i+2}, ...a_p, a_1, a_2, ..., a_i)$.

a) Check that this is indeed an action of $C$ on $S$. Hint: show that if in a group we have $a_1 a_2 \dots a_n = e$ then $a_2 \dots a_n a_1 = e$.

b) Show that the number of elements in $S$ equals $|G|^{p-1}$ (note that any choice of $a_1, \dots, a_{p-1}$ uniquely determines $a_p$).

c) Show that an element in $S$ has orbit consisting of only 1 element (i.e. is a fixed point for this action) if and only if it is of the form $(g, ..., g)$ for some $g \in G$ such that $g^p = e$.

d) Note that the cardinality of $S$ is divisible by $p$ and the size of each orbit is either 1 or $p$. Conclude that the number of orbits with 1 element is divisible by $p$.

e) Conclude that $G$ has an element of order $p$.

**Solution.** a) We need to verify that if $(a_1, \dots, a_p) \in S$ then $(a_{i+1}, a_{i+2}, \dots, a_p, a_1, a_2, \dots, a_i) \in S$. We will use the fact that in any group $G$ if $ab = e$ then $ba = e$. Thus

$$e = a_1 \dots a_p = (a_1 \dots a_i)(a_{i+1} a_{i+2} \dots a_p)$$

so

$$e = (a_{i+1} a_{i+2} \dots a_p)(a_1 \dots a_i) = a_{i+1} a_{i+2} \dots a_p, a_1 a_2 \dots a_i.$$

This means that $(a_{i+1}, a_{i+2}, \dots, a_p, a_1, a_2, \dots, a_i) \in S$. The verification that $*$ is an action is now straightforward.

b) Note that $(a_1, \ldots, a_p) \in S$ if and only if $a_p = (a_1 \ldots a_{p-1})^{-1}$. Thus elements in $S$ are in bijection with sequences of length $p-1$ consisting of elements from $G$. We have $|G|^{p-1}$ such sequences, so $|S| = |G|^{p-1}$.

c) If $(a_1, \ldots, a_p)$ is a fixed point that $(a_1, \ldots, a_p) = f * (a_1, \ldots, a_p) = (a_2, \ldots, a_p, a_1)$. Thus $a_i = a_{i+1}$ for all $i$, so $(a_1, \ldots, a_p) = (g, \ldots, g)$ and $g^p = e$. Conversely, if $g^p = e$ then $(g, \ldots, g) \in S$ is a fixed point.

d) Since $p||G|$ and $|S| = |G|^{p-1}$, we have $p||S|$. Note that the size of each orbit divides the size of the group acting, which is $p$. Thus each orbit has either size 1 or $p$ and the orbits partition $S$. If we have $r$ orbits of size 1, i.e. we have $r$ fixed points, then $|S| = r +$ multiple of $p$. Since $p$ divides $S$, we conclude that $p|r$.

e) Note that $(e, \ldots, e)$ is a fixed point, so $r > 0$. This means that there are at least $p$ different fixed points. Thus there is $g \neq e$ such that $g^p = e$. Any such $g$ has order $p$.

We proved the following theorem:

**Cauchy's Theorem.** If $G$ is a finite group and $p$ is a prime such that $p||G|$ then $G$ has an element of order $p$.

**The following problems are optional.**

**Problem 5.** Let $p$ be a prime number and let $P = \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \ldots \times \mathbb{Z}_{p^{m_k}}$ for some $m_1 \geq m_2 \geq \ldots \geq m_k \geq 1$.

a) Consider the subgroup $P_1 = \{a \in P : a^p = e\}$. Show that $P_1$ has $p^k$ elements. Thus $k$ is uniquely determined by $P$.

b) Consider the subgroup $P_2 = \{a \in P : a^{p^2} = e\}$. Show that $P_2$ has $p^{2k-r}$ elements, where $r$ is the number of indexes $i$ such that $m_i = 1$. Conclude that $r$ is uniquely determined by $P$.

c) Prove that $P/P_1 \cong \mathbb{Z}_{p^{m_1-1}} \times \mathbb{Z}_{p^{m_2-1}} \times \ldots \times \mathbb{Z}_{p^{m_{k-r}-1}}$.

d) Use c) and induction to prove that the sequence $m_1, m_2, \ldots, m_k$ is uniquely determined by $P$.

**Solution.** Note that in the group $P = \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \ldots \times \mathbb{Z}_{p^{m_k}}$ the group operation is addition so $a^n$ means $a + a + \ldots + a = na$.
We also note that if $A =< g >$ is a cyclic group of order $n$ and $k|n$ then $\{a \in A : a^k = e\}$ is a cyclic subgroup of order $k$ consisting of the elements $g^{ni/k}$ for $i = 1, 2, \ldots, k$. We denote this subgroup by $A[k]$. Furthermore, $A/A[k]$ is a cyclic group of order $n/k$.
Thus $\mathbb{Z}_{p^m}[p^k]$ is a cyclic group of order $p^k$ if $k < m$ and it is the whole group $\mathbb{Z}_{p^m}$ if $k \geq m$.

a) We have $(a_1, ..., a_k) \in P_1$ if and only if $(pa_1, \ldots, pa_k) = (0, \ldots, 0)$, i.e. if and only if $a_i \in \mathbb{Z}_{p^{m_i}}[p]$ for all $i$. Thus $P_1 = \mathbb{Z}_{p^{m_1}}[p] \times \mathbb{Z}_{p^{m_2}}[p] \times \ldots \times \mathbb{Z}_{p^{m_k}}[p]$ is a product of $k$ cyclic groups of order $p$, so $|P_1| = p^k$.

b) In the same way as in a) we see that

$$P_2 = \mathbb{Z}_{p^{m_1}}[p^2] \times \mathbb{Z}_{p^{m_2}}[p^2] \times \ldots \times \mathbb{Z}_{p^{m_k}}[p^2].$$

Now if $m_i = 1$ then $\mathbb{Z}_{p^{m_i}}[p^2] = \mathbb{Z}_{p^{m_i}}$ has $p$ elements and if $m_i > 1$ then $\mathbb{Z}_{p^{m_i}}[p^2]$ is cyclic of order $p^2$. Thus $|P_2| = (p^2)^{k-r} p^r = p^{2k-r}$.

c) We have

$$P/P_1 = (\mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \ldots \times \mathbb{Z}_{p^{m_k}})/(\mathbb{Z}_{p^{m_1}}[p] \times \mathbb{Z}_{p^{m_2}}[p] \times \ldots \times \mathbb{Z}_{p^{m_k}}[p]) \cong$$

$$(\mathbb{Z}_{p^{m_1}}/\mathbb{Z}_{p^{m_1}}[p]) \times (\mathbb{Z}_{p^{m_2}}/\mathbb{Z}_{p^{m_2}}[p]) \times \ldots \times (\mathbb{Z}_{p^{m_k}}/\mathbb{Z}_{p^{m_k}}[p]) \cong \mathbb{Z}_{p^{m_1-1}} \times \mathbb{Z}_{p^{m_2-1}} \times \ldots \times \mathbb{Z}_{p^{m_{k-r}-1}}.$$

We used here the isomorphism $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$and the fact that $\mathbb{Z}_{p^m}/\mathbb{Z}_{p^m}[p]$ is a cyclic group of order $p^{m-1}$, hence isomorphic to $\mathbb{Z}_{p^{m-1}}$.

d) Let $P = \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \ldots \times \mathbb{Z}_{p^{m_k}}$ and $Q = \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \ldots \times \mathbb{Z}_{p^{n_l}}$ be two abelian groups of order $p^N$, where $m_1 \geq m_2 \geq \ldots \geq m_k \geq 1$ and $n_1 \geq n_2 \geq \ldots \geq n_l \geq 1$. We need to prove that if the groups $P$ and $Q$ are isomorphic then $k = l$ and $m_i = n_i$ for all $i$. We prove it by induction on $N$. When $N = 1$ then clearly $k = l = 1$ and $m_1 = n_1 = 1$. Suppose that the result is true for all abelian $p$-groups of order less than $p^N$ and consider two isomorphic groups $P$ and $Q$ of order $p^N$. Any isomorphism from $P$ to $Q$ induces an isomorphisms of $P_1$ and $Q_1$, $P_2$ and $Q_2$ and $P/P_1$ and $Q/Q_1$. By part a), $P_1$ has $p_k$ elements and $Q_1$ has $p^l$ elements. It follows that $k = l$. Let $r$ be the numbers of $i$ such that $m_i = 1$ and $s$ the number of $i$ such that $n_i = 1$. By part b), $P_2$ has $p^{2k-r}$ elements and $Q_2$ has $p^{2l-s}$ elements. Thus $2k - r = 2l - s$. Since $k = l$, we get $r = s$. Thus $m_{k-r+j} = n_{k-r+j} = 1$ for $j = 1, \ldots, r$. Since the groups $P/P_1$ and $Q/Q_1$ are isomorphic and have order smaller than $p^N$, from part c) and the inductive assumption we conclude that $m_i - 1 = n_i - 1$ for $i = 1, \ldots, k - r$. Thus $m_i = n_i$ for all $i$, which completes our proof of the inductive step.